

DOCKET NO.: 255147US6PCT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Susumu SENSU

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP03/13752

INTERNATIONAL FILING DATE: October 28, 2003

FOR: RECORDING SYSTEM AND METHOD, RECORDING APPARATUS AND METHOD,  
INPUT DEVICE AND METHOD, PLAYBACK SYSTEM AND METHOD, PLAYBACK  
APPARATUS AND METHOD, RECORDING MEDIUM, AND PROGRAM

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119  
AND THE INTERNATIONAL CONVENTION**

Commissioner for Patents  
Alexandria, Virginia 22313


Sir:

In the matter of the above-identified application for patent, notice is hereby given that  
the applicant claims as priority:

<b><u>COUNTRY</u></b>	<b><u>APPLICATION NO</u></b>	<b><u>DAY/MONTH/YEAR</u></b>
Japan	2002-336754	20 November 2002

Certified copies of the corresponding Convention application(s) were submitted to the  
International Bureau in PCT Application No. PCT/JP03/13752. Receipt of the certified  
copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been  
acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,  
OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



Gregory J. Maier  
Attorney of Record  
Registration No. 25,599  
Surinder Sachar  
Registration No. 34,423

Customer Number

**22850**

(703) 413-3000  
Fax No. (703) 413-2220  
(OSMMN 08/03)

## PATENT COOPERATION TREATY

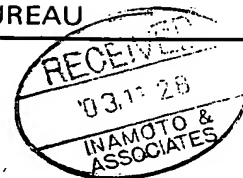
PCT

NOTIFICATION CONCERNING  
SUBMISSION OR TRANSMITTAL  
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

From the INTERNATIONAL BUREAU

To:

INAMOTO, Yoshio  
711 Building 4F, 11-18, Nishi-  
Shinjuku 7-chome  
Shinjuku-ku, Tokyo 160-0023  
Japan

Date of mailing (day/month/year) 20 November 2003 (20.11.03)	<b>IMPORTANT NOTIFICATION</b>
Applicant's or agent's file reference 584-S03P1336	
International application No. PCT/JP03/13752	International filing date (day/month/year) 28 October 2003 (28.10.03)
International publication date (day/month/year) Not yet published	Priority date (day/month/year) 20 November 2002 (20.11.02)
Applicant SONY CORPORATION et al	

- The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).
- This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.
- An asterisk(\*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, **the attention of the applicant is directed to Rule 17.1(c)** which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.
- The letters "NR" appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, **the attention of the applicant is directed to Rule 17.1(c)** which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

<u>Priority date</u>	<u>Priority application No.</u>	<u>Country or regional Office or PCT receiving Office</u>	<u>Date of receipt of priority document</u>
20 Nove 2002 (20.11.02)	2002-336754	JP	14 Nove 2003 (14.11.03)

The International Bureau of WIPO  
34, chemin des Colombettes  
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 338.70.10

Authorized officer

Rémy CALCAGNO (Fax 338 7010)

Telephone No. (41-22) 338 9018

10/500851

PCT/JP03/13752

10 Rec'd PCT/JP03

16 JUL 2004

日 本 国 特 許 庁

28.10.03

JAPAN PATENT OFFICE

REC'D 14 NOV 2003

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2002年11月20日

出 願 番 号  
Application Number: 特願2002-336754  
[ST. 10/C]: [JP2002-336754]

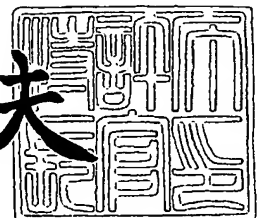
出 願 人  
Applicant(s): ソニー株式会社

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2003年 8月14日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 0290580314

【提出日】 平成14年11月20日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/14

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 千秋 進

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100082131

【弁理士】

【氏名又は名称】 稲本 義雄

【電話番号】 03-3369-6479

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要



【書類名】 明細書

【発明の名称】 記録システムおよび方法、記録装置および方法、入力装置および方法、再生装置および方法、記録媒体、並びにプログラム

【特許請求の範囲】

【請求項 1】 入力装置と記録装置がバスを介して接続された記録システムにおいて、

前記入力装置は、入力されたコンテンツを保護するか否かを判断する判断手段を備え、

前記記録装置は、前記判断手段により判断された結果に基づいて、前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かを示す保護情報を、前記コンテンツとともに記録媒体に記録する記録手段を備える

ことを特徴とする記録システム。

【請求項 2】 前記記録手段は、前記コンテンツの所定の単位ごとに前記保護情報を記録する

ことを特徴とする請求項 1 に記載の記録システム。

【請求項 3】 前記所定の単位は、2048 バイトである  
ことを特徴とする請求項 2 に記載の記録システム。

【請求項 4】 前記記録装置は、前記判断手段により前記コンテンツを保護すると判断された場合、前記記録媒体の ID と記録媒体鍵を作用させて前記コンテンツを暗号化する暗号化手段をさらに備える

ことを特徴とする請求項 1 に記載の記録システム。

【請求項 5】 前記記録装置は、前記判断手段により前記コンテンツを保護しないと判断された場合、少なくとも、前記記録媒体の記録媒体鍵を作用させて前記コンテンツを暗号化する暗号化手段をさらに備える

ことを特徴とする請求項 1 に記載の記録システム。

【請求項 6】 前記入力装置および前記記録装置は、それぞれ相互に認証する認証手段をさらに備える

ことを特徴とする請求項 1 に記載の記録システム。

【請求項 7】 前記入力装置は、前記判断手段により前記コンテンツを保護

すると判断された場合、前記バスへの前記コンテンツの送出前に、前記コンテンツを暗号化する第1の暗号化手段をさらに備え、

前記記録装置は、前記判断手段により前記コンテンツを保護すると判断された場合、前記記録手段による前記コンテンツの記録前に、前記コンテンツを暗号化する第2の暗号化手段をさらに備える

ことを特徴とする請求項1に記載の記録システム。

【請求項8】 前記判断手段により前記コンテンツを保護しないと判断された場合、前記第1の暗号化手段は、前記バスへの前記コンテンツの送出前に、前記コンテンツを暗号化することを禁止する

ことを特徴とする請求項7に記載の記録システム。

【請求項9】 入力装置と記録装置がバスを介して接続された記録システムの記録方法において、

前記入力装置は、入力されたコンテンツを保護するか否かを判断し、

前記記録装置は、判断された結果に基づいて、前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を、前記コンテンツとともに記録媒体に記録する

ことを特徴とする記録方法。

【請求項10】 記録媒体に情報を記録する記録装置において、

バスを介して接続された他の装置と相互に認証を行う認証手段と、

前記他の装置から前記バスを介して供給される第1の暗号化方法により暗号化されたコンテンツを復号する復号手段と、

前記復号手段により復号された前記コンテンツとともに、前記バス上での伝送において保護すべきコンテンツであることを示す保護情報を、前記記録媒体に記録する記録手段と

を備えることを特徴とする記録装置。

【請求項11】 前記復号された前記コンテンツを、第2の暗号化方法により暗号化する暗号化手段をさらに備える

ことを特徴とする請求項10に記載の記録装置。

【請求項12】 前記暗号化手段は、前記記録媒体のIDと記録媒体鍵を作

用させて前記復号されたコンテンツを暗号化する

ことを特徴とする請求項 11 に記載の記録装置。

【請求項 13】 前記記録手段は、前記他の装置から前記バスを介して供給された前記コンテンツが、前記第 1 の暗号方法により暗号化されていないコンテンツの場合、前記コンテンツを、前記バス上での伝送において保護すべきコンテンツでないことを示す保護情報とともに記録する

ことを特徴とする請求項 10 に記載の記録装置。

【請求項 14】 記録媒体に情報を記録する記録装置の記録方法において、バスを介して接続された他の装置と相互に認証を行う認証ステップと、

前記他の装置から前記バスを介して供給される暗号化されたコンテンツを復号する復号ステップと、

前記復号ステップの処理により復号された前記コンテンツとともに、前記バス上での伝送において保護すべきコンテンツであることを示す保護情報を、前記記録媒体に記録する記録ステップと

を含むことを特徴とする記録方法。

【請求項 15】 記録媒体に情報を記録する記録装置用のプログラムであって、

バスを介して接続された他の装置と相互に認証を行う認証ステップと、

前記他の装置から前記バスを介して供給される暗号化されたコンテンツを復号する復号ステップと、

前記復号ステップの処理により復号された前記コンテンツとともに、前記バス上での伝送において保護すべきコンテンツであることを示す保護情報を、前記記録媒体に記録する記録ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 16】 記録媒体に情報を記録する記録装置のプログラムであって、

バスを介して接続された他の装置と相互に認証を行う認証ステップと、

前記他の装置から前記バスを介して供給される暗号化されたコンテンツを復号

する復号ステップと、

前記復号ステップの処理により復号された前記コンテンツとともに、前記バス上での伝送において保護すべきコンテンツであることを示す保護情報を、前記記録媒体に記録する記録ステップと

を含むことを特徴とするプログラム。

【請求項 17】 コンテンツが入力される入力装置において、

バスを介して接続された記録装置と相互に認証を行う認証手段と、

入力された前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かに応じて、前記コンテンツを第 1 の暗号化方法で暗号化する第 1 の暗号化手段と、

前記第 1 の暗号化手段により暗号化された前記コンテンツを、前記バスを介して前記記録装置に供給する供給手段と

を備えることを特徴とする入力装置。

【請求項 18】 前記第 1 の暗号化手段により暗号化された前記コンテンツを、第 2 の暗号化方法で暗号化する第 2 の暗号化手段を

さらに備えることを特徴とする請求項 17 に記載の入力装置。

【請求項 19】 前記第 1 の暗号化手段および前記第 2 の暗号化手段のうちの一方は、記録媒体の ID と記録媒体鍵を作用させて前記コンテンツを暗号化する

ことを特徴とする請求項 18 に記載の入力装置。

【請求項 20】 コンテンツが入力される入力装置の入力方法において、

バスを介して接続された記録装置と相互に認証を行う認証ステップと、

入力された前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かに応じて、前記コンテンツを暗号化する暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記コンテンツを、前記バスを介して前記記録装置に供給する供給ステップと

を含むことを特徴とする入力方法。

【請求項 21】 コンテンツが入力される入力装置用のプログラムであって

、

バスを介して接続された記録装置と相互に認証を行う認証ステップと、  
入力された前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かに応じて、前記コンテンツを暗号化する暗号化ステップと、  
前記暗号化ステップの処理により暗号化された前記コンテンツを、前記バスを介して前記記録装置に供給する供給ステップと  
を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 22】 コンテンツが入力される入力装置のプログラムであって、バスを介して接続された記録装置と相互に認証を行う認証ステップと、  
入力された前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かに応じて、前記コンテンツを暗号化する暗号化ステップと、  
前記暗号化ステップの処理により暗号化された前記コンテンツを、前記バスを介して前記記録装置に供給する供給ステップと  
を含むことを特徴とするプログラム。

【請求項 23】 コンテンツを記録媒体から再生し、他の装置にバスを介して供給する再生装置において、

前記記録媒体から前記コンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生手段と、

前記再生手段により再生された前記保護情報に基づいて、前記バスを介しての前記他の装置への前記コンテンツの出力を制御する出力制御手段と

を備えることを特徴とする再生装置。

【請求項 24】 前記保護情報は、前記コンテンツの所定の単位ごとに記録されている

ことを特徴とする請求項 23 に記載の再生装置。

【請求項 25】 前記所定の単位は、2048 バイトであることを特徴とする請求項 24 に記載の再生装置。

【請求項 26】 前記他の装置を認証する認証手段と、  
前記コンテンツを暗号化する暗号化手段とをさらに備え、

前記保護情報により前記コンテンツが前記バス上の伝送において保護すべきコンテンツであることが示され、かつ、前記認証手段により前記他の装置が認証された場合、前記暗号化手段は、前記バスへの前記コンテンツの送出前に、前記コンテンツを暗号化する

ことを特徴とする請求項 23 に記載の再生装置。

【請求項 27】 前記保護情報により前記コンテンツが前記バス上の伝送において保護すべきコンテンツであることが示され、かつ、前記認証手段により前記他の装置が認証されない場合、前記出力制御手段は、前記バスへの前記コンテンツの出力を禁止する

ことを特徴とする請求項 26 に記載の再生装置。

【請求項 28】 コンテンツを記録媒体から再生し、他の装置にバスを介して供給する再生装置の再生方法において、

前記記録媒体から前記コンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、

前記再生ステップの処理により再生された前記保護情報に基づいて、前記バスを介しての前記他の装置への前記コンテンツの出力を制御する出力制御ステップと

を含むことを特徴とする再生方法。

【請求項 29】 コンテンツを記録媒体から再生し、他の装置にバスを介して供給する再生装置用のプログラムであって、

前記記録媒体から前記コンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、

前記再生ステップの処理により再生された前記保護情報に基づいて、前記バスを介しての前記他の装置への前記コンテンツの出力を制御する出力制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 30】 コンテンツを記録媒体から再生し、他の装置にバスを介して供給する再生装置のプログラムにおいて、

前記記録媒体から前記コンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、

前記再生ステップの処理により再生された前記保護情報に基づいて、前記バスを介しての前記他の装置への前記コンテンツの出力を制御する出力制御ステップと

を含むことを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、記録システムおよび方法、記録装置および方法、入力装置および方法、再生装置および方法、記録媒体、並びにプログラムに関し、特に、保護の要否に基づいて、コンテンツを柔軟に保護することができるようにした記録システムおよび方法、記録装置および方法、入力装置および方法、再生装置および方法、記録媒体、並びにプログラムに関する。

【0002】

【従来の技術】

記録再生装置（例えば、CD-RWドライブなど）においては、ディスクに記録または再生を行う場合、コンテンツを保護するために、正当な記録再生制御と不正コピーの防止が求められている。

【0003】

例えば、特許文献1には、ユーザデータとユーザコントロールデータにより構成されるデータフォーマットを用いて、ディスクに記録または再生を行うことが提案されている。

【0004】

このようなデータフォーマットにおいては、そのユーザデータ部分に、ディスクに固有のIDであるディスクIDを作用させた鍵で暗号化して記録することに

よりコンテンツが不当なコピーから保護される。

【0005】

また、特許文献2には、図1に示される記録再生装置1が開示されている。

【0006】

図1の例においては、記録再生装置1は、ドライブ11、AVボード12および専用バス13により構成される。ドライブ11は、記録再生処理部21を有し、AVボード12は、AVコンテンツ処理部31、コンテンツ保護部32、入力部33および出力部34を有している。

【0007】

記録再生処理部21は、光ディスク41が装着されると、光ディスク41に固有のディスクIDおよびRKB (Renewal Key Block) を取得し、専用バス13を介して、AVボード12のコンテンツ保護部32に供給する。コンテンツ保護部32は、取得したディスクIDおよびRKBから得たディスク鍵を作用させた鍵を生成し、記憶する。

【0008】

AVコンテンツ処理部31は、アンテナなどにより構成される入力部33を介して受信された著作権を保護する必要があるコンテンツを、コンテンツ保護部32に供給する。コンテンツ保護部32は、予め記憶されているディスクIDおよびRKBから得たディスク鍵などを作用させた鍵でコンテンツを暗号化し、保護すべきコンテンツとして、専用バス13を介して、記録再生処理部21に供給する。記録再生処理部21は、暗号化されたコンテンツを受信し、光ディスク41に記録する。

【0009】

また、記録再生処理部21は、光ディスク41から所定の暗号化されたコンテンツを再生し、専用バス13を介して、コンテンツ保護部32に供給する。コンテンツ保護部32は、暗号化されたコンテンツを、ディスクIDおよびRKBから得たディスク鍵を作用させた鍵で復号し、AVコンテンツ処理部31に供給する。AVコンテンツ処理部31は、復号されたコンテンツを、例えば、MPEG (Moving Picture Experts Group) 方式でデコードし、再生する。出力部34は、再



生されたコンテンツを出力する。

#### 【0010】

以上のように、ドライブ11とAVボード12間においては、記録再生装置1内の専用バス13を介しているため、外部からアクセスされることはなく、ディスクIDまたはRKBを利用して、コンテンツを保護することができる。

#### 【0011】

図1の変形例として、図2に示されるような、記録再生装置51が考えられる。尚、図2において、図1における場合と対応する部分には対応する符号を付しており、その説明は繰り返しになるので省略するが、図2の例の場合、ドライブ11とAVボード12がバス61（汎用バス）を介して分離されている（例えば、家庭内LAN(Local Area Network)などで分離されている）。

#### 【0012】

したがって、図2の例においては、バス61にディスクIDおよびRKBがそのまま流れてしまうため、これらが盗用される危険が生じる。例えば、コンテンツを記録する場合、HDD(Hard Disk Drive)71をバス61に接続することにより、バス61上にある「ディスクID」、「RKB」および「ディスクIDおよびRKBから得たディスク鍵を用いて暗号化されたコンテンツ」が吸い上げられ（モニターされ）、HDD71にコピーされてしまう。

#### 【0013】

図2の例の場合、HDD71には、以上のようにして吸い上げられた、16BのディスクID、数MBのRKB、および20GBの暗号化コンテンツ、並びに、数KBのプログラムが記憶されている。HDD71により、これらの「ディスクID」、「RKB」および「ディスクIDおよびRKBから得たディスク鍵を用いて暗号化されたコンテンツ」が、AVボード12に与えられると、正当な光ディスク41から再生されたものの識別ができないため、AVボード12においては、コンテンツの再生が許容されてしまう。

#### 【0014】

以上のように、吸い上げた「ディスクID」、「RKB」および「ディスクIDおよびRKBから得たディスク鍵を用いて暗号化されたコンテンツ」を、AV

ボード12に対して与える「なりすましドライブ」または「なりすましプログラム」は、再生実行型装置またはプログラムとして、一般的に流通されてしまう恐れがある。

#### 【0015】

したがって、ドライブ11とAVボード12が、バス61を介して分離している構成の記録再生装置51においては、正当なディスクでなくても、HDD71のように、何らかのメディアにコピーされ、流通されてしまう恐れがある。

#### 【0016】

そこで、図3に示されるような相互認証を行う記録再生装置81が提案される。図3の例においては、ドライブ11に相互認証部91が設けられ、AVボード12に相互認証部92が設けられ、それらの間で相互認証処理が実行されることにより共有された共通鍵を用いて暗号化することで、コンテンツの送受信が行われる。

#### 【0017】

これにより、記録再生装置1または記録再生装置51で記録された光ディスクと互換性があり、かつ、相互認証機能を有しないHDD71においては、「ディスクID」、「RKB」および「ディスクIDおよびRKBから得たディスク鍵を用いて暗号化されたコンテンツ」がコピーされたとしても、その復号ができないので、実質的にコピーを不可能にすることができる。したがって、上述した「なりすましドライブ」または「なりすましプログラム」を防止することができる。

#### 【0018】

##### 【特許文献1】

特表2002-521789号公報

##### 【特許文献2】

特開2002-84271号公報

#### 【0019】

##### 【発明が解決しようとする課題】

しかしながら、最近、暗号化コンテンツをフリーで提供するという超流通用途

のため、あるいは、P C (Personal Computer) ストレージ用途のために、保護する必要がないコンテンツは、ユーザから見てコピー可能なように、バス 13 上では暗号化せずに記録、再生できるようにし、かつ、保護すべきコンテンツは、実質的にコピー防止できるようにすることが望まれている。

#### 【0020】

しかしながら、現在、一般の P C の H D D 7 1 には、相互認証処理を実行する機能が備えられていないため、記録再生装置 8 1 においては、H D D 7 1 には、保護すべき特定のコンテンツだけでなく、P C ストレージ用途のための保護不要のコンテンツまでもコピーすることができなくなってしまうといった課題があった。

#### 【0021】

本発明はこのような状況に鑑みてなされたものであり、保護の要不要に基づいて、コンテンツを柔軟に保護することができるようにするものである。

#### 【0022】

##### 【課題を解決するための手段】

本発明の記録システムは、入力装置は、入力されたコンテンツを保護するか否かを判断する判断手段を備え、記録装置は、判断手段により判断された結果に基づいて、コンテンツがバス上での伝送において保護すべきコンテンツであるか否かを示す保護情報を、コンテンツとともに記録媒体に記録する記録手段を備えることを特徴とする。

#### 【0023】

記録手段は、コンテンツの所定の単位ごとに保護情報を記録するようにすることができる。

#### 【0024】

所定の単位は、2048 バイトであるようにすることができる。

#### 【0025】

記録装置は、判断手段によりコンテンツを保護すると判断された場合、記録媒体の I D と記録媒体鍵を作用させてコンテンツを暗号化する暗号化手段をさらに備えるようにすることができる。

**【 0 0 2 6 】**

記録装置は、判断手段によりコンテンツを保護しないと判断された場合、少なくとも、記録媒体の記録媒体鍵を作用させてコンテンツを暗号化する暗号化手段をさらに備えるようにすることができる。

**【 0 0 2 7 】**

入力装置および記録装置は、それぞれ相互に認証する認証手段をさらに備えるようにすることができる。

**【 0 0 2 8 】**

入力装置は、判断手段によりコンテンツを保護すると判断された場合、バスへのコンテンツの送出前に、コンテンツを暗号化する第 1 の暗号化手段をさらに備え、記録装置は、判断手段によりコンテンツを保護すると判断された場合、記録手段によるコンテンツの記録前に、コンテンツを暗号化する第 2 の暗号化手段をさらに備えるようにすることができる。

**【 0 0 2 9 】**

判断手段によりコンテンツを保護しないと判断された場合、第 1 の暗号化手段は、バスへのコンテンツの送出前に、コンテンツを暗号化することを禁止するようにすることができる。

**【 0 0 3 0 】**

本発明の第 1 の記録方法は、入力装置は、入力されたコンテンツを保護するか否かを判断し、記録装置は、判断された結果に基づいて、コンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を、コンテンツとともに記録媒体に記録することを特徴とする。

**【 0 0 3 1 】**

本発明の記録装置は、バスを介して接続された他の装置と相互に認証を行う認証手段と、他の装置からバスを介して供給される第 1 の暗号化方法により暗号化されたコンテンツを復号する復号手段と、復号手段により復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報を、記録媒体に記録する記録手段とを備えることを特徴とする。

**【 0 0 3 2 】**

復号されたコンテンツを、第2の暗号化方法により暗号化する暗号化手段をさらに備えるようにすることができる。

#### 【0033】

暗号化手段は、記録媒体のIDと記録媒体鍵を作用させて復号されたコンテンツを暗号化するようにすることができる。

#### 【0034】

記録手段は、他の装置からバスを介して供給されたコンテンツが、第1の暗号方法により暗号化されていないコンテンツの場合、コンテンツを、バス上での伝送において保護すべきコンテンツでないことを示す保護情報とともに記録するようにすることができる。

#### 【0035】

本発明の第2の記録方法は、バスを介して接続された他の装置と相互に認証を行う認証ステップと、他の装置からバスを介して供給される暗号化されたコンテンツを復号する復号ステップと、復号ステップの処理により復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報を、記録媒体に記録する記録ステップとを含むことを特徴とする。

#### 【0036】

本発明の第1の記録媒体のプログラムは、バスを介して接続された他の装置と相互に認証を行う認証ステップと、他の装置からバスを介して供給される暗号化されたコンテンツを復号する復号ステップと、復号ステップの処理により復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報を、記録媒体に記録する記録ステップとを含むことを特徴とする。

#### 【0037】

本発明の第1のプログラムは、バスを介して接続された他の装置と相互に認証を行う認証ステップと、他の装置からバスを介して供給される暗号化されたコンテンツを復号する復号ステップと、復号ステップの処理により復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報を、記録媒体に記録する記録ステップとを含むことを特徴とする。

**【 0 0 3 8 】**

本発明の入力装置は、バスを介して接続された記録装置と相互に認証を行う認証手段と、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツを第 1 の暗号化方法で暗号化する第 1 の暗号化手段と、第 1 の暗号化手段により暗号化されたコンテンツを、バスを介して記録装置に供給する供給手段とを備えることを特徴とする。

**【 0 0 3 9 】**

第 1 の暗号化手段により暗号化されたコンテンツを、第 2 の暗号化方法で暗号化する第 2 の暗号化手段をさらに備えるようにすることができる。

**【 0 0 4 0 】**

第 1 の暗号化手段および第 2 の暗号化手段のうちの一方は、記録媒体の ID と記録媒体鍵を作用させてコンテンツを暗号化するようにすることができる。

**【 0 0 4 1 】**

本発明の入力方法は、バスを介して接続された記録装置と相互に認証を行う認証ステップと、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツを暗号化する暗号化ステップと、暗号化ステップの処理により暗号化されたコンテンツを、バスを介して記録装置に供給する供給ステップとを含むことを特徴とする。

**【 0 0 4 2 】**

本発明の第 2 の記録媒体のプログラムは、バスを介して接続された記録装置と相互に認証を行う認証ステップと、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツを暗号化する暗号化ステップと、暗号化ステップの処理により暗号化されたコンテンツを、バスを介して記録装置に供給する供給ステップとを含むことを特徴とする。

**【 0 0 4 3 】**

本発明の第 2 のプログラムは、バスを介して接続された記録装置と相互に認証を行う認証ステップと、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツを暗号化する暗号化ステップと、暗号化ステップの処理により暗号化されたコンテンツを、バスを介して記録

装置に供給する供給ステップとを含むことを特徴とする。

【0044】

本発明の再生装置は、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生手段と、再生手段により再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力を制御する出力制御手段とを備えることを特徴とする。

【0045】

保護情報は、コンテンツの所定の単位ごとに記録されているようにすることができる。

【0046】

所定の単位は、2048バイトであるようにすることができる。

【0047】

他の装置を認証する認証手段と、コンテンツを暗号化する暗号化手段とをさらに備え、保護情報によりコンテンツがバス上の伝送において保護すべきコンテンツであることが示され、かつ、認証手段により他の装置が認証された場合、暗号化手段は、バスへのコンテンツの送出前に、コンテンツを暗号化するようにすることができる。

【0048】

保護情報によりコンテンツがバス上の伝送において保護すべきコンテンツであることが示され、かつ、認証手段により他の装置が認証されない場合、出力制御手段は、バスへのコンテンツの出力を禁止するようにすることができる。

【0049】

本発明の再生方法は、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、再生ステップの処理により再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力を制御する出力制御ステップとを含むことを特徴とする。

【0050】

本発明の第3の記録媒体のプログラムは、記録媒体からコンテンツ、およびコ

コンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、再生ステップの処理により再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力を制御する出力制御ステップとを含むことを特徴とする。

#### 【0051】

本発明のプログラムは、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、再生ステップの処理により再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力を制御する出力制御ステップとを含むことを特徴とする。

#### 【0052】

第1の本発明においては、入力装置により、入力されたコンテンツを保護するか否かが判断され、判断された結果に基づいて、記録装置により、コンテンツがバス上での伝送において保護すべきコンテンツであるか否かを示す保護情報が、コンテンツとともに記録媒体に記録される。

#### 【0053】

入力装置は、独立した装置であっても良いし、入力記録装置の入力処理を行うブロックであってもよい。

#### 【0054】

記録装置は、独立した装置であっても良いし、記録再生装置の記録処理を行うブロックであってもよい。

#### 【0055】

第2の本発明においては、バスを介して接続された他の装置と相互に認証が行われる。そして、他の装置からバスを介して供給される暗号化されたコンテンツが復号され、復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報が、記録媒体に記録される。

#### 【0056】

第3の本発明においては、バスを介して接続された記録装置と相互に認証が行われる。そして、入力されたコンテンツがバス上での伝送において保護すべきコ



ンテンツであるか否かに応じて、コンテンツが暗号化され、暗号化されたコンテンツが、バスを介して記録装置に供給される。

【0057】

第4の本発明においては、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報が再生され、再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力が制御される。

【0058】

再生装置は、独立した装置であっても良いし、記録再生装置の再生処理を行うブロックであってもよい。

【0059】

【発明の実施の形態】

以下、図を参照して本発明の実施の形態について説明する。

【0060】

図4は、本発明を適用した記録再生装置101の構成例を表している。家庭内LAN(Local Area Network)に代表されるバス113には、ドライブ111、AVボード112、およびHDD(hard disk drive)114が接続されている。なお、ドライブ111、AVボード112、およびHDD114は、独立に販売されるものであり、ユーザにより、バス113に接続されるものである。

【0061】

この例の場合、ドライブ111およびAVボード112は、それぞれ自分自身の秘密鍵と公開鍵を有している。この公開鍵および秘密鍵の登録は、例えば、メーカーにより出荷時に、あらかじめ行なわれている。なお、公開鍵は、図示せぬ認証局が発行した電子署名の中に記憶される。ドライブ111およびAVボード112の間におけるコンテンツの転送には、例えば、RSAなどの公開鍵暗号化方式が使用される。なお、秘密鍵とそれに対応する公開鍵は、一方の鍵に基づいて生成された暗号文を他方の鍵を用いて復号できる関係にある。

【0062】

ドライブ111は、他の装置（図4の例の場合、AVボード112）との相互

認証処理を実行する相互認証部121、ドライブ111の各部の制御を実行する入出力制御部122、および、ドライブ111に装着された光ディスク141に、コンテンツの記録または再生を実行する記録再生処理部123により構成される。

#### 【0063】

AVボード112は、他の装置（図4の例の場合、ドライブ111）との相互認証処理を実行する相互認証部131、光ディスク141に記憶するコンテンツを暗号化するコンテンツ保護部132、アンテナなどにより構成される入力部134を介してコンテンツを受信したり、コンテンツをデコードし、出力部135に出力するAVコンテンツ処理部133により構成される。

#### 【0064】

ドライブ111の相互認証部121は、AVボード112の相互認証部131との間で相互認証処理を実行する。具体的に説明すると、ドライブ111とAVボード112が接続され、それぞれの電源がオンされたとき、AVボード112の相互認証部131は、内蔵する乱数発生部（図示せず）の乱数に基づいて、共通鍵を生成し、生成された共通鍵をドライブ111の公開鍵で暗号化し、AVボード112の秘密鍵により暗号化された共通鍵への署名を生成する。また、相互認証部131は、内蔵するメモリから、認証局から予め取得され、記憶されているAVボード電子証明書を読み出し、暗号化された共通鍵、AVボード112による共通鍵への署名、およびAVボード電子証明書を、バス113を介して、ドライブ111に送信する。

#### 【0065】

ドライブ111の相互認証部121は、これらを受信し、暗号化された共通鍵をドライブ111の秘密鍵で復号して共通鍵（第1の共通鍵）を取得するとともに、AVボード電子証明書を、認証局から予め取得された認証局公開鍵で復号し、AVボード112が正当なAVボードであることを確認する。また、相互認証部121は、復号されたAVボード電子証明書から取得されたAVボード112の公開鍵により、共通鍵への署名を復号して共通鍵（第2の共通鍵）を取得する。ドライブ111の相互認証部121は、第1の共通鍵と第2の共通鍵を比較し

、両者が等しいと判断された場合、バス 1 1 3 上で、共通鍵が改ざんされていないと判断する。これにより、共通鍵が、ドライブ 1 1 1 と A V ボード 1 1 2 との間で共有されたことになる。

#### 【 0 0 6 6 】

以上のようにして、ドライブ 1 1 1 の相互認証部 1 2 1 は、A V ボード 1 1 2 の相互認証部 1 3 1 との間で相互認証処理を実行し、A V ボード 1 1 2 を相互認証する。これにより、相互認証部 1 2 1 および相互認証部 1 3 1 は、お互いに、この共通鍵を用いて、コンテンツを暗号化して送信したり、受信したコンテンツを復号することができる。

#### 【 0 0 6 7 】

一方、HDD 1 1 4 は、A V ボード 1 1 2 の相互認証部 1 3 1 のような相互認証機能を有していない。したがって、HDD 1 1 4 は、バス 1 1 3 上に流れても問題がない（保護しなくてもよい）フリーコンテンツ（保護する必要がないコンテンツ）の送受信をドライブ 1 1 1 と実行することができる。

#### 【 0 0 6 8 】

A V ボード 1 1 2 の A V コンテンツ処理部 1 3 3 は、入力部 1 3 4 を介して放送信号（暗号化またはスクランブルされているコンテンツに対応する信号）を受信すると、予め記憶されている鍵（放送信号を送信する機器と共有している鍵）で暗号化またはスクランブルされているコンテンツを復号し、コンテンツ保護部 1 3 2 に供給する。

#### 【 0 0 6 9 】

また、A V コンテンツ処理部 1 3 3 は、入力されたコンテンツが、暗号化またはスクランブルされているか否かに基づいて、入力されたコンテンツが保護すべきコンテンツであるか否かという判断を実行する。なお、このコンテンツ（放送信号）に、例えば、コンテンツのコピーを制限するために、「Copy Free(コピー可)」，「Copy Once(一世代のみコピー可)」，「No More Copy (この世代以上のコピー不可)」，「Copy Prohibited(コピー禁止)」というコピー世代管理情報（Copy generation management information）を示す、例えば、C G M S (Copy Generation Management System) 信号のような C C I (Copy Control Information)

が付加されている場合、このコピー世代管理情報が「Copy Free」のときには、入力されたコンテンツが保護すべきコンテンツではないとし、「Copy Once」、  
「No More Copy」または「Copy Prohibited」のときには、入力されたコンテンツが保護すべきコンテンツであると判断するようにしてもよい。

#### 【0070】

コンテンツ保護部132は、コンテンツをAVコンテンツ処理部133より入力し、AVコンテンツ処理部133によりそのコンテンツが保護すべきコンテンツであると判断された場合、相互認証部131より供給された光ディスク141のRKBを作用させたディスク鍵を取得し、取得されたディスク鍵および光ディスク141のディスクIDに基づいて、ブロック鍵を生成する。コンテンツ保護部132は、このブロック鍵を用いて、光ディスク141上におけるコンテンツ保護のために、保護すべきコンテンツを暗号化し、相互認証部131に供給する。

#### 【0071】

相互認証部131は、コンテンツ保護部132により暗号化されたコンテンツを、バス113上におけるコンテンツ保護のために、ドライブ111との共通鍵で暗号化し、バス113を介してドライブ111に出力する。

#### 【0072】

なお、AVコンテンツ処理部133によりコンテンツが保護すべきコンテンツではないと判断された場合、コンテンツ保護部132および相互認証部131は、そのコンテンツを暗号化せず、バス113を介してドライブ111に出力する。

#### 【0073】

ドライブ111の相互認証部121は、バス113を介してAVボード112からコンテンツを入力する。また、相互認証部121は、入力されたコンテンツが暗号化されている場合、ドライブ111との共通鍵で復号し、復号したコンテンツを記録再生処理部123に供給する。

#### 【0074】

入出力制御部122は、相互認証部121に入力されたコンテンツが、AVボ

ード112の相互認証部131により、AVボード112との共通鍵で暗号化されているか否か（すなわち、AVコンテンツ処理部133により保護すべきコンテンツであると判断されたか否か）に基づいて、そのコンテンツがバス113上で保護されるべきコンテンツであるか否かを判断する。そして、入出力制御部122は、入力されたコンテンツがバス113上で保護されるべきコンテンツであるか否か、かつ、相互認証部121によりAVボード112との間で相互認証がされたか否かに基づいて、記録再生処理部123によるコンテンツの記録制御を行う。

#### 【0075】

また、入出力制御部122は、入力されたコンテンツが保護されるべきコンテンツであるか否か、かつ、相互認証部121によりAVボード112との間で相互認証がされたか否かに基づいて、記録再生処理部123を制御し、光ディスク141に記録されているディスクIDおよびRKB (Renewal Key Block)などの光ディスク141のディスク情報を再生させる。

#### 【0076】

記録再生処理部123は、光ディスク141にコンテンツを記録する場合、入出力制御部122の指示に基づいて、記録するコンテンツが、バス113上で保護すべきコンテンツまたはバス113上で保護不要のコンテンツであるかを示す保護情報を生成し、その保護情報をコンテンツとともに光ディスク141に記録する。

#### 【0077】

図5は、光ディスク141に記録されるデータフォーマットの構成例を示している。

#### 【0078】

このデータフォーマットにおいては、1フレーム当り2K（2048）バイトで32フレームのユーザデータ201と、1フレーム当り18バイトで32フレームのユーザコントロールデータ202により、32セクタが構成されている。

#### 【0079】

ユーザデータ201は、コンテンツのデータなどにより構成される。このユー

ザデータ201は、各フレームに、4つ(4バイト)のEDC(エラー検出コード)が付加され、図6に示されるようなデータフレーム203が構成される。

#### 【0080】

図6の例においては、1つのデータフレームは、2052バイトで構成される。すなわち、1つのデータフレームは、Ud0乃至Ud2047の番号が振られた2048個のユーザデータバイト、およびed2048乃至ed2051の番号が振られた4つのEDCにより構成されている。

#### 【0081】

このデータフレーム203が32フレーム分集められ、16×9バイトに配列された物理アドレス204に基づいて、図7に示されるようなスクランブルデータフレーム205として構成される。

#### 【0082】

図7の例の場合、1番目の(図中、左端の列の)フレームは、d(0, 0), d(1, 0), ..., d(2051, 0)の番号が振られた2052バイトにより構成され、2番目(図中、左端から2番目の列の)のフレームは、d(0, 1), d(1, 1), ..., d(2051, 1)の番号が振られた2052バイトにより構成される。同様に、F-1番目のフレームは、d(0, F), d(1, F), ..., d(2051, F)の番号が振られた2052バイトにより構成され、32番目の(図中、右端の列の)フレームは、d(0, 31), d(1, 31), ..., d(2051, 31)の番号が振られた2052バイトにより構成される。

#### 【0083】

以上のようなスクランブルデータフレーム205から、216行304列のデータブロック206が形成される。データブロック206に、32行のパリティを付加することにより、LDC(長距離コード:誤り訂正)ブロック207が形成される。LDCブロック207から、152列496行のLDCクラスタ208が形成される。LDCクラスタ208は、それぞれが38列の4つのLDC列209-1乃至209-4に分割され、後述するBIS列213-1乃至213-3とによりECCクラスタ221を構成する。

#### 【0084】

一方、この記録再生装置 101 により付加されるアドレスおよび制御データを説明する。ユーザコントロールデータ（論理アドレスおよび制御データ）202 は、図 8 に示されるように、 $32 \times 18$  バイトに配列される。

#### 【0085】

図 8 の例の場合、1 番目の（図中、左端の列の）フレームは、UC (0, 0) , UC (1, 0) , …, UC (17, 0) の番号が振られた 18 バイトにより構成され、2 番目の（図中、左端から 2 番目の列の）フレームは、UC (0, 1) , UC (1, 1) , …, UC (17, 1) の番号が振られた 18 バイトにより構成される。同様に、S-1 番目のフレームは、UC (0, S) , UC (1, S) , …, UC (17, S) の番号が振られた 18 バイトにより構成され、32 番目の（図中、右端の列の）フレームは、UC (0, 31) , UC (1, 31) , …, UC (17, 31) の番号が振られた 2052 バイトにより構成される。

#### 【0086】

上述したように、このデータフォーマットにおいては、各フレーム単位で、2K (2048) バイトのユーザデータ 201 につき、18 バイトのユーザコントロールデータ 202 が対応している。そこで、このユーザデータ 201 (2K バイト) に記録されるデータ（コンテンツ）に対して、バス 113 上で保護すべきコンテンツであるか否かを示す保護情報が生成され、そのユーザデータ 201 に対応するユーザコントロールデータ 202 (18 バイト) の先頭バイト UC (0, S) の最下位ビットに格納される。

#### 【0087】

例えば、記録するコンテンツがバス 113 上で保護すべきコンテンツである場合、保護情報として、ユーザコントロールデータ 202 (18 バイト) の先頭バイト UC (0, S) の最下位ビットに、「0」が生成され、記録される。また、記録するコンテンツがバス 113 上で保護する必要がないコンテンツである場合、保護情報として、ユーザコントロールデータ 202 (18 バイト) の先頭バイト UC (0, S) の最下位ビットに、「1」が生成され、記録される。なお、既存のデータフォーマットにおいては、ユーザコントロールデータ 202 (18 バイト) の先頭バイト UC (0, S) の最下位ビットには、もともと「0」が格納

されている（未使用とされている）。したがって、既存のデータフォーマットにより記録した保護すべきコンテンツに対しても、バス 1 1 3 上で保護すべき情報が格納されていることになるので、既存のものとの互換性を保持することができる。

#### 【0 0 8 8】

保護を要するコンテンツの保護情報を「1」とし、保護不要のコンテンツの保護情報を「0」とすることも可能である。しかしながら、そのようにすると、既存のコンテンツはすべてバス 1 1 3 上で保護不要のコンテンツとなってしまう、実質的に保護することができなくなってしまう。そこで、保護を要するコンテンツの保護情報を「0」とし、保護不要のコンテンツの保護情報を「1」とするのが好ましい。

#### 【0 0 8 9】

また、物理アドレス 2 0 4 は、1 6 × 9 バイトに配列される。この物理アドレス 2 0 4 は、ディスク 1 4 1 上の物理的距離に関係する。

#### 【0 0 9 0】

3 2 × 1 8 バイトのユーザコントロールデータ 2 0 2 から、物理アドレス 2 0 4 に基づいて、2 4 列 × 3 0 行のアクセスブロック 2 1 0 が形成される。アクセスブロック 2 1 0 は、3 2 行のパリティが付加され、B I S（バースト指示サブコード）ブロック 2 1 1 が形成される。B I S ブロック 2 1 1 は、3 列 × 4 9 6 行の B I S クラスタ 2 1 2 に配列される。

#### 【0 0 9 1】

B I S クラスタ 2 1 2 は、L D C 列 2 0 9 - 1 乃至 2 0 9 - 4 の間に、それぞれが 1 列の 3 つの B I S 列 2 1 3 - 1 乃至 2 1 3 - 3 に充填され、1 5 5 列 × 4 9 6 行の E C C クラスタ 2 2 1 が形成される。この E C C クラスタ 2 2 1 から、4 5 チャンネルビットのデータ(data)および 1 チャンネルビットのコントロールデータ(dc contr.)の 4 2 個の組み合わせにより物理クラスタ 2 2 2 が形成され、光ディスク 1 4 1 に記録される。

#### 【0 0 9 2】

この物理クラスタ 2 2 2 は、1 9 3 2 チャンネルビット（1 2 8 8 データビッ



ト) の 496 の記録フレームにグループ化されている。なお、物理クラスタ 22 の最初のデータ(data)のうち、20 チャンネルビットは、同期ビット群(Frame Sync)とされる。

#### 【0093】

以上のようにして、記録再生処理部 123 により、記録するコンテンツがバス 113 上で保護すべきコンテンツである場合、保護情報として、「0」が生成（格納）され、記録するコンテンツがバス 113 上で保護不要のコンテンツである場合、保護情報として、「1」が生成（格納）され、生成された保護情報がユーザコントロールデータ 202 に記録される。

#### 【0094】

このデータフォーマットの光ディスク 141 に記録されたコンテンツを再生する場合の誤り訂正動作としては、一般的には、BIS の誤り訂正動作を行い、BIS の誤り訂正動作の結果を LDC の誤り訂正動作を行う際の消失情報として用いる。したがって、LDC の誤り訂正動作が終わって、ユーザデータを出力できるようになる前に、BIS の誤り訂正動作は終了しているため、BIS に含まれるユーザコントロールデータは、すでに得られている。したがって、ユーザコントロールデータを用いて、ユーザデータの出力制御は可能である。

#### 【0095】

以上のように、光ディスク 141 に記録された保護情報は、記録再生処理部 123 により、光ディスク 141 に記録されたコンテンツを再生する場合、コンテンツよりも先に再生されるので、この再生された保護情報に基づいて、入出力制御部 122 は、バス 113 へのコンテンツの出力の制御を行う。

#### 【0096】

例えば、入出力制御部 122 は、相互認証部 121 により AV ボード 112 との間で相互認証がされたか否か、および、再生されたコンテンツがバス 113 上で保護されるべきコンテンツであるか（保護情報が「0」であるか）否かに基づいて、相互認証部 121 によるコンテンツのバス 113 への出力制御を行う。相互認証部 121 は、この入出力制御部 122 の制御に基づいて、再生されたコンテンツを、ドライブ 111 との共通鍵で暗号化し、バス 113 を介して AV ボー

ド112に出力する。

【0097】

このドライブ111の相互認証部121により暗号化されたコンテンツが入力されると、AVボード112の相互認証部131は、そのコンテンツを復号し、コンテンツ保護部132に供給する。

【0098】

コンテンツ保護部132は、相互認証部131によりAVボード112との共通鍵を用いて復号されたコンテンツを、さらに、光ディスク141のディスクIDおよびディスク鍵を作用させたブロック鍵により復号し、AVコンテンツ処理部133に供給する。AVコンテンツ処理部133は、復号されたコンテンツを、例えば、MPEG (Moving Picture Experts Group) 方式でデコードし、再生する。出力部135は、再生されたコンテンツを出力する。

【0099】

以上のように、AVボード112は、ドライブ111と相互認証されているので、著作権などにより保護されるべきコンテンツ（保護すべきコンテンツ）または保護不要のコンテンツをお互いに送受信することができる。

【0100】

一方、例えば、HDD114により保護されるべきコンテンツがドライブ111に送信されてきたとしても、HDD114は、ドライブ111により相互認証されないため、そのコンテンツは、ドライブ111において保護不要のコンテンツとしてであれば処理される。すなわち、この記録再生装置101において、コピーフリーのコンテンツのみを扱う相互認証しないストレージは許可される。

【0101】

以上のようにして、この記録再生装置101においては、著作権などによりコンテンツの保護が必要か否かによって、コンテンツの暗号化またはコンテンツの汎用バスへの出力が柔軟に制御される。

【0102】

図9は、コンテンツ保護部132の構成例を示している。なお、図9においては、説明の便宜上、コンテンツ保護部132と光ディスク141しか記載されて

いないが、実際には、コンテンツ保護部 132 と光ディスク 141 との間では、図 4 に示されるように、相互認証部 131、バス 113、相互認証部 121 および記録再生処理部 123 が、それぞれの処理を実行している。

#### 【0103】

図 9 の例においては、コンテンツ保護部 132 は、RKB 処理部 252、鍵生成部 253 および暗号化部 254 により構成される。

#### 【0104】

RKB 処理部 252 は、AV コンテンツ処理部 133 からの入力されたコンテンツが保護されるべきコンテンツであるか否かの情報に基づいて、光ディスク 141 から供給された RKB、コンテンツ保護部 132 に予め記憶されているデバイス ID およびデバイス鍵を作用させて、ディスク鍵を取得する（このディスク鍵の取得処理については、特許文献 2 に開示されており、さらに、図 10 乃至図 12 を参照して詳しく後述する）。

#### 【0105】

鍵生成部 253 は、RKB 処理部 252 により取得されたディスク鍵、および、光ディスク 141 から供給されたディスク ID および、コンテンツ保護部 132 に記憶されている記録情報（例えば、ブロックシード、タイトルキーまたは記録モードなどの記録時に使用する情報）を作用させて、ブロック鍵を生成する。

#### 【0106】

暗号化部 254 は、光ディスク 141 より供給されるコンテンツが暗号化されている場合、鍵生成部 253 により生成されたブロック鍵を用いて、暗号化コンテンツを復号し、AV コンテンツ処理部 133 に出力する。暗号化部 254 は、光ディスク 141 より供給されるコンテンツが暗号化されていない場合、そのコンテンツをそのまま、AV コンテンツ処理部 133 に出力する。

#### 【0107】

また、暗号化部 254 は、AV コンテンツ処理部 133 からの入力されたコンテンツが保護されるべきコンテンツであるか否かの情報に基づいて、AV コンテンツ処理部 133 より供給されるコンテンツが保護すべきコンテンツである場合、光ディスク 141 上でのコンテンツ保護のために、鍵生成部 253 により生成

されたブロック鍵を用いて、コンテンツを暗号化し、光ディスク 141 に供給する。暗号化部 254 は、AV コンテンツ処理部 133 より供給されるコンテンツが保護不要のコンテンツである場合、コンテンツをそのまま（暗号化せずに）、光ディスク 141 に供給する。

#### 【0108】

次に、ディスク鍵の取得処理に使用される RKB について詳しく説明する。図 10 は、本発明の記録再生装置 101 の鍵の配布構成を示す図である。図 10 の最下段に示すナンバー 0 乃至 15 が個々の記録再生装置（デバイス）に対応する。すなわち、図 10 に示される木（ツリー）構造の各葉（リーフ：leaf）がそれぞれ記録再生装置に相当する。

#### 【0109】

各デバイス 0 乃至 15 は、製造時（出荷時）に、予め設定されている初期ツリーにおける、自分のリーフからルート（最上段）に至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーを自身で格納する。図 10 の最下段に示す K0000 乃至 K1111 が、各デバイス 0 乃至 15 にそれぞれ割り当てられたリーフキーであり、最上段の KR から、最下段から 2 番目の節（ノード）に記載されたキー KR 乃至 K111 がノードキーである。

#### 【0110】

図 10 の例においては、例えば、デバイス 0 は、リーフキー K0000 と、ノードキー K000, K00, K0, KR を所有する。デバイス 5 は、K0101, K010, K01, K0, KR を所有する。デバイス 15 は、K1111, K111, K11, K1, KR を所有する。なお、図 10 のツリーには、デバイスが 16 個のみ記載され、ツリー構造も 4 段構成の均衡のとれた左右対称構成として示されているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を有するようにしてもよい。

#### 【0111】

また、図 10 のツリー構造に含まれる各記録再生装置には、様々な記録媒体、例えば、DVD、CD、MD（商標）、メモリスティック（登録商標）などを使用する様々なタイプの記録再生装置が含まれている。さらに、様々なアプリケー

ションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に、図10に示されるようなキー配布構成が適用される。

#### 【0112】

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば、図10の点線で囲まれた部分、すなわち、デバイス0, 1, 2, 3は、同一の記録媒体を用いる1つのグループとして設定される。このツリー構造においては、1つのグループに含まれる4つのデバイス0, 1, 2, 3はノードキーとして共通のキーK00, K0, KRを保有する。このノードキー共有構成を利用することにより、例えば共通のマスター鍵をデバイス0, 1, 2, 3のみに提供することが可能となる。

#### 【0113】

例えば、共通に保有するノードキーK00自体をマスター鍵として設定すれば、新たな鍵送付を実行することなく、デバイス0, 1, 2, 3のみに共通のマスター鍵の設定が可能である。また、新たなマスター鍵KmasterをノードキーK00で暗号化した値Enc(K00, Kmaster)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kmaster)を解いてマスター鍵Kmasterを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

#### 【0114】

また、ある時点tにおいて、デバイス3の所有する鍵K0011, K001, K00, K0, KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0, 1, 2, 3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキーK001, K00, K0, KRをそれぞれ新たな鍵：K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世

代 (Generation) :  $t$  の更新キーであることを示す。

#### 【0 1 1 5】

更新キーの配布処理について説明する。キーの更新は、例えば、図 1 1 A に示す R K B (Renewal Key Block) と呼ばれるブロックデータによって構成されるテーブルを、たとえばネットワーク、あるいは記録媒体に格納してデバイス 0, 1, 2 に供給することによって実行される。

#### 【0 1 1 6】

図 1 1 A に示す R K B には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図 1 1 は、図 1 0 に示されるツリー構造中のデバイス 0, 1, 2 において、世代  $t$  の更新ノードキーを配布することを目的として形成されたブロックデータの例を示す。上述したように、デバイス 0, デバイス 1 は、更新ノードキーとして  $K(t) 0 0, K(t) 0, K(t) R$  が必要であり、デバイス 2 は、更新ノードキーとして  $K(t) 0 0 1, K(t) 0 0, K(t) 0, K(t) R$  が必要である。

#### 【0 1 1 7】

図 1 1 A の R K B に示されるように、R K B には複数の暗号化キーが含まれる。最下段の暗号化キーは、 $E n c (K 0 0 1 0, K(t) 0 0 1)$  である。これはデバイス 2 の持つリーフキー  $K 0 0 1 0$  によって暗号化された更新ノードキー  $K(t) 0 0 1$  であり、デバイス 2 は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t) 0 0 1$  を得ることができる。また、復号により得た  $K(t) 0 0 1$  を用いて、図 1 1 A の下から 2 段目の暗号化キー  $E n c (K(t) 0 0 1, K(t) 0 0)$  が復号可能となり、更新ノードキー  $K(t) 0 0$  を得ることができる。以下、順次、図 1 1 A の上から 2 段目の暗号化キー  $E n c (K(t) 0 0, K(t) 0)$  を復号し、更新ノードキー  $K(t) 0$ 、図 1 1 A の上から 1 段目の暗号化キー  $E n c (K(t) 0, K(t) R)$  を復号し、 $K(t) R$  が得られる。

#### 【0 1 1 8】

一方、ノードキー  $K 0 0 0$  は更新する対象に含まれておらず、デバイス 0, 1 が、更新ノードキーとして必要とするのは、 $K(t) 0 0, K(t) 0, K(t)$

) Rである。デバイス 0, 1 は、図 11 A の上から 3 段目の暗号化キー Enc (K 0 0 0, K (t) 0 0) を復号し、K (t) 0 0 を取得し、以下、図 11 A の上から 2 段目の暗号化キー Enc (K (t) 0 0, K (t) 0) を復号し、更新ノードキー K (t) 0 を得、図 11 A の上から 1 段目の暗号化キー Enc (K (t) 0, K (t) R) を復号し、K (t) R を得る。このようにして、デバイス 0, 1, 2 は更新した鍵 K (t) R を得ることができる。なお、図 11 A のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

#### 【0119】

図 10 に示すツリー構造の上位 2 段のノードキー K 0, K R の更新が不要であり、ノードキー K 0 0 のみの更新処理が必要である場合には、図 11 B の R K B を用いることで、更新ノードキー K (t) 0 0 をデバイス 0, 1, 2 に配布することができる。

#### 【0120】

図 11 B に示す R K B は、例えば、特定のグループにおいて共有する新たなマスター鍵を配布する場合に利用可能である。具体例として、図 10 に、点線で示すグループ内のデバイス 0, 1, 2, 3 がある記録媒体を用いており、新たな共通のマスター鍵 K (t) master が必要であるとする。このとき、デバイス 0, 1, 2, 3 の共通のノードキー K 0 0 を更新した K (t) 0 0 を用いて新たな共通の更新マスター鍵 K (t) master を暗号化したデータ Enc (K (t), K (t) master) を、図 11 B に示す R K B とともに配布する。この配布により、デバイス 4 など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

#### 【0121】

すなわち、デバイス 0, 1, 2, 3 は R K B を処理して得た K (t) 0 0 を用いて上記暗号文を復号すれば、t 時点でのマスター鍵 K (t) master を得ることが可能になる。

#### 【0122】

以上においては、R K B を用いて、各記録再生装置に対してマスター鍵を伝送

し、これを用いて記録再生装置がデータの記録、再生を行う例を説明したが、本発明においては、上述したマスター鍵として、記録媒体のみに限定されたものであるディスク鍵が使用される。このディスク鍵は、図12に示されるように、記録媒体のRKB(Renewal Key Block)を用いて生成される。なお、ディスク鍵K(t) mediaは、マスター鍵をその記録媒体のみに限定したものであり、基本的な構成は、上述したマスター鍵と同様であるため、その説明を省略する。

#### 【0123】

図12の例の場合、デバイス0が、記録媒体に格納されている世代:t 時点のRKBと、自分があらかじめ格納しているリーフキーK0000と、ノードキーK000, K00を用いて更新ノードキーK(t)00を生成し、それを用いて更新ディスク鍵K(t) mediaを得る様子を示している。ここで得たK(t) mediaは、その記録媒体のデータの記録、再生時に使用される。

#### 【0124】

なお、図12におけるプレ記録世代番号(Generation #n)は、ディスク鍵においてはマスター鍵のように世代の新旧という概念はないので必須ではなくオプションとして設定される。

#### 【0125】

以上のようにして、光ディスク141からのRKB、コンテンツ保護部132のデバイスID(例えば、図10のデバイス0)、デバイス鍵(例えば、図10のデバイス0におけるリーフキーK0000)およびノードキー(図10のデバイス0におけるK000, K00, ...)などに基づいて、ディスク鍵が取得される。このディスク鍵の取得処理は、例えば、コンテンツの記録もしくは再生のために、光ディスク141が記録再生装置101のドライブ111に装着された際に実行されるようにしてもよいし、または、光ディスク141が装着されており、コンテンツの記録もしくは再生を指示した際に実行されるようにしてもよい。

#### 【0126】

次に、図13のフローチャートを参照して、記録再生装置101のAVボード112の相互認証処理について説明する。

#### 【0127】



ドライブ111とAVボード112が接続され、それぞれの電源がオンされたとき、ステップS11において、AVボード112の相互認証部131は、内蔵する乱数発生部の乱数に基づいて、共通鍵を生成する。ステップS12において、相互認証部131は、生成された共通鍵をドライブ111の公開鍵で暗号化する。ステップS13において、相互認証部131は、AVボード112の秘密鍵により暗号化された共通鍵への署名を生成する。ステップS14において、相互認証部131は、内蔵するメモリより、図示せぬ認証局から予め取得され、記憶されているAVボード電子証明書を読み出す。ステップS15において、相互認証部131は、暗号化された共通鍵、AVボード112による共通鍵への署名、およびAVボード電子証明書を、バス113を介して、ドライブ111に送信する。

#### 【0128】

このようにして、AVボード112から、暗号化された共通鍵、AVボード112による共通鍵への署名、およびAVボード電子証明書がドライブ111に送信される。このAVボード112の相互認証処理に対応するドライブ111の相互認証処理を、図14のフローチャートを参照して説明する。

#### 【0129】

ステップS31において、ドライブ111の相互認証部121は、受信したAVボード電子証明書を、予め取得してあるか、その都度取得する認証局公開鍵に基づいて復号する。ステップS32において、相互認証部121は、ステップS31において復号されたAVボード電子証明書に基づいて、AVボード112が正当なAVボードであるか否かを判断する。AVボード電子証明書が復号できなかったり、改ざんされている場合には、ステップS32において、AVボード112が正当なAVボードではないと判断され、処理は終了する。

#### 【0130】

ステップS32において、AVボード112が正当なAVボードであると判断された場合、AVボード電子証明書を復号することによりAVボード112の公開鍵が得られる。相互認証部121は、ステップS33において、暗号化されている共通鍵を、ドライブ111の秘密鍵を用いて復号する。ステップS34にお

いて、相互認証部 121 は、AV ボード 112 による共通鍵への署名を、AV ボード 112 の公開鍵を用いて復号する。

#### 【0131】

ステップ S 35 において、相互認証部 121 は、ステップ S 33 において復号された共通鍵と、署名に平文で添付されている共通鍵を比較し、両者が一致するか否かを判断する。これにより、その共通鍵が正当な共通鍵であるか否かが判定される。ステップ S 35 において、共通鍵と、署名の共通鍵が一致すると判断された場合、相互認証部 121 は、AV ボード 112 から正当な共通鍵が送信されてきたと判定し、ステップ S 36 において、共通鍵を記憶する。一方、ステップ S 35 において、共通鍵と、署名の共通鍵が一致しないと判断された場合、相互認証部 121 は、AV ボード 112 とドライブ 111 との間において、共通鍵が改ざんされているとし、処理を終了する。

#### 【0132】

以上のようにして、ドライブ 111 と AV ボード 112 との間で、相互認証が行われ、共通鍵が共有されている状態において、これ以降の処理が実行される。

#### 【0133】

なお、説明は省略するが、さらに、ドライブ 111 の相互認証部 121 が、AV ボード 112 から取得した共通鍵をドライブ 111 の公開鍵で暗号化したもの、それに対するドライブ 111 による署名、およびドライブ電子証明書を、AV ボード 112 に送信し、AV ボード 112 に認証させるようにしてもよい。

#### 【0134】

次に、図 15 のフローチャートを参照して、記録再生装置 101 の AV ボード 112 の記録要求処理について説明する。

#### 【0135】

ステップ S 101 において、AV コンテンツ処理部 133 は、コンテンツが入力されるまで待機している。AV コンテンツ処理部 133 は、アンテナなどにより構成される入力部 134 を介して放送信号（コンテンツに対応する信号）を受信すると、ステップ S 101 において、コンテンツが入力されたと判断し、ステップ S 102 において、入力されたコンテンツが暗号化またはスクランブルされ

ているか否かに基づいて、入力されたコンテンツが保護すべきコンテンツであるか否かを判断する。

#### 【0136】

ステップS102において、AVコンテンツ処理部133は、そのコンテンツが保護すべきコンテンツであると判断した場合、暗号化またはスクランブルされているコンテンツを、予め記憶されている鍵（放送信号を送信する機器と共有している鍵）で復号し、ステップS103において、AVコンテンツ処理部133は、コンテンツ保護部132にブロック鍵生成処理を実行させる。このブロック鍵生成処理を、図16のフローチャートを参照して説明する。なお、図16のAVボード112におけるブロック鍵生成処理に対応するドライブ111のドライブ情報取得処理も、図17のフローチャートを参照して、合わせて説明する。

#### 【0137】

ステップS121において、RKB処理部252は、光ディスク141のディスク情報（例えば、ディスクIDおよびRKB）の読み出しの要求を、ドライブ111に出力する。具体的には、RKB処理部252は、光ディスク141のディスクIDおよびRKBの読み出しの要求を、相互認証部131に出力する。相互認証部131は、ディスクIDおよびRKBの読み出しの要求を、バス113を介して、ドライブ111の相互認証部121に出力する。

#### 【0138】

ステップS141において、ドライブ111の相互認証部121は、バス113を介して、AVボード112からの光ディスク141のディスクIDおよびRKBの読み出しの要求を受信する。

#### 【0139】

ステップS142において、入出力制御部122は、相互認証部121からの情報に基づいて、このディスクIDおよびRKBの読み出しの要求をするAVボード112が、ドライブ111において相互認証されているか否かを判断する。ステップS142において、AVボード112が、ドライブ111において相互認証されていないと判断された場合、ドライブ111のディスク情報再生処理は終了する。これにより、不正な装置からの要求は拒絶される。

## 【0140】

上述したように、AVボード112は、ドライブ111において相互認証されているので、ステップS142において、AVボード112が、ドライブ111において相互認証されていると判断される。この場合、ステップS143において、記録再生処理部123は、光ディスク141に記録されているディスクIDおよびRKBを再生し、相互認証部121に供給する。

## 【0141】

ステップS144において、相互認証部121は、記録再生処理部123により供給されたディスクIDおよびRKBを、AVボード112との共通鍵を用いて暗号化し、バス113を介して、AVボード112に出力する。

## 【0142】

ステップS122において、AVボード112の相互認証部131は、バス113を介して、暗号化されているディスクIDおよびRKBを受信し、ドライブ111との共通鍵を用いて復号し、RKB処理部251に供給する。

## 【0143】

ステップS123において、RKB処理部251は、供給されたRKBと内蔵するメモリに予め記憶されているデバイスIDおよびデバイスキーを作用させて、ディスク鍵を取得する。具体的には、RKB処理部251は、供給されたRKBと、自身がメモリに記憶しているデバイスID（例えば、図10のデバイス0）、デバイスキー（例えば、図10のデバイス0におけるリーフキーK0000）、およびノードキー（例えば、図10のデバイス0におけるK000, K00, K0, KR）を用いて、プレ記録世代情報Generation #n（例えば、図12におけるt）時点でのノード00の鍵K(t)00を計算する。そして、RKB処理部251は、供給されたRKBの中から、ディスク鍵K(t)mediaを、鍵K(t)00で暗号化した暗号文Enc(K(t)00, K(t)media)を取得し、これを復号して、ディスク鍵K(t)mediaを取得する。

## 【0144】

ステップS124において、鍵生成部253は、相互認証部131より供給されたディスクID、ステップS123において取得されたディスク鍵、および、

コンテンツ保護部 132 の記録情報などを作用させて、ブロック鍵を生成し、暗号化部 254 に内蔵されるメモリなどに記憶する。

#### 【0145】

以上のようにしてブロック鍵が生成されるので、図 15 のステップ S104 において、暗号化部 254 は、AV コンテンツ処理部 133 より供給されたコンテンツを、ステップ S124 において生成されたブロック鍵で暗号化し、相互認証部 131 に出力する。

#### 【0146】

相互認証部 131 は、ステップ S105 において、ステップ S104 においてブロック鍵で暗号化されたコンテンツを、さらに、ドライブ 111 との共通鍵を用いて、暗号化し、ステップ S106 において、バス 113 を介してドライブ 111 に出力する。

#### 【0147】

一方、ステップ S102 において、AV コンテンツ処理部 133 より入力されたコンテンツが保護不要のコンテンツであると判断された場合、そのコンテンツは、暗号化部 254 において暗号化する（光ディスク 141 上で保護する）必要がなく、相互認証部 131 においても暗号化する（バス 113 上で保護する）必要がないため、ステップ S103 乃至 S105 の処理は、スキップされる。すなわち、暗号化部 254 は、そのコンテンツを暗号化させずに（生データのままで）、相互認証部 131 に出力する。ステップ S106 において、相互認証部 131 は、暗号化されていないコンテンツを、バス 113 を介して、ドライブ 111 に出力する。

#### 【0148】

以上のようにして、AV ボード 112 からは、保護すべきコンテンツは、RKB およびディスク ID を作用させたブロック鍵で暗号化され、さらに、ドライブ 111 との共通鍵で一時的に暗号化され、バス 113 に出力される。また、保護不要のコンテンツは、生データのまま、バス 113 に出力される。これに対応して実行されるドライブ 111 の記録処理を、図 18 のフローチャートを参照して説明する。

## 【0149】

ステップS161において、ドライブ111の相互認証部121は、バス113を介して、AVボード112よりコンテンツを受信する。

## 【0150】

ステップS162において、入出力制御部122は、相互認証部121からの情報に基づいて、コンテンツを入力してきた装置が、ドライブ111において相互認証されているか否かを判断する。ステップS162において、AVボード112が、ドライブ111において相互認証されていると判断された場合、ステップS163において、入出力制御部122は、相互認証部121に入力されたコンテンツが共通鍵で暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス113上で保護すべきコンテンツの記録コマンドであるかを判断する。

## 【0151】

ステップS163において、このコンテンツの記録コマンドが、バス113上で保護すべきコンテンツの記録コマンドであると判断された場合、ステップS164において、入出力制御部122は、相互認証部121を制御し、受信したコンテンツを、AVボード112との共通鍵で復号させる。したがって、いま、このコンテンツは、ディスクIDおよびRKBを作用させたブロック鍵にのみ暗号化された状態となる。

## 【0152】

入出力制御部122は、記録再生処理部123を制御し、ステップS165において、このコンテンツに対応するユーザコントロールデータのUC(0, S)に、バス113上で保護すべきコンテンツであるという保護情報「0」を生成、格納させ、ステップS168において、ブロック鍵で暗号化された状態のコンテンツとともに、光ディスク141に記録させる。

## 【0153】

一方、例えば、相互認証部を有しないHDD114に記憶されているコンテンツが入力される。この場合、ステップS161において、HDD114からコンテンツが、バス113を介して、相互認証部121に受信される。HDD114

は、相互認証部を有しないので、ステップS162において、コンテンツを入力してきた装置が、ドライブ111において相互認証されていないと判断され、処理は、ステップS166に進む。ステップS166において、入出力制御部122は、相互認証部121に入力されたコンテンツが共通鍵で暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス113上で保護すべきコンテンツの記録コマンドであるか否かを判断する。

#### 【0154】

ステップS163において、または、ステップS166において、入力されたコンテンツの記録コマンドが、バス113上で保護不要のコンテンツの記録コマンドであると判断された場合、ステップS167において、入出力制御部122は、記録再生処理部123を制御し、コンテンツに対応するユーザコントロールデータのUC(0, S)に、バス113上で保護不要のコンテンツであるという保護情報「1」を生成(格納)させ、生成された保護情報を、ステップS168において、暗号化されていないコンテンツとともに、光ディスク141に記録させる。

#### 【0155】

また、ステップS166において、入力されたコンテンツの記録コマンドが、バス113上で保護すべきコンテンツの記録コマンドであると判断された場合、エラーとなり、ドライブ111の記録処理は、強制的に終了される。したがって、ドライブ111においては、相互認証されないHDD114からのコンテンツは、バス113上で保護すべきコンテンツとしては記録されない。

#### 【0156】

以上のように、相互認証されているAVボード112からの保護すべきコンテンツは、バス113上で保護すべきコンテンツであるという保護情報「0」とともに光ディスク141に記録される。この場合、保護すべきコンテンツは、ディスクIDおよびRKBを作用させたブロック鍵により暗号化されている。また、相互認証されているAVボード112からの保護不要のコンテンツ、または、相互認証されていないHDD114からの保護不要のコンテンツは、バス113上で保護不要のコンテンツであるという保護情報「1」とともに光ディスク141

に記憶される。この場合、保護不要のコンテンツは、暗号化されていない。

#### 【0157】

以上のようにして格納された保護情報は、次に説明するドライブ111のコンテンツ再生処理により再生され、利用される。図19のフローチャートを参照して、ドライブ111のコンテンツ再生処理について説明する。

#### 【0158】

ユーザは、光ディスク141に記録されている保護すべきコンテンツを、AVボード112の出力部135から出力させるために、図示せぬ入力部などを介して、AVボード112に、コンテンツの再生コマンドを入力する。AVボード112の相互認証部131は、バス113を介して、ドライブ111に再生コマンドを送信してくるので、ステップS191において、相互認証部121は、AVボード112からの再生コマンドを入力する。

#### 【0159】

ステップS192において、入出力制御部122は、相互認証部121からの情報に基づいて、コンテンツを出力する機器（いまの場合、AVボード112）が、ドライブ111において相互認証されているか否かを判断する。ステップS192において、AVボード112が相互認証されていると判断された場合、ステップS193において、入出力制御部122は、AVボード112からの再生コマンドが、保護すべきコンテンツの再生コマンドであるか否かを判断する。

#### 【0160】

ステップS193において、AVボード112からの再生コマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、ステップS194において、記録再生処理部123は、光ディスク141から指示されたコンテンツを再生する。

#### 【0161】

図5を参照して上述したように、光ディスク141に記録された保護情報（ユーザコントロールデータ）は、コンテンツを再生する場合、そのコンテンツよりも先に再生されるので、ステップS195において、入出力制御部122は、そのコンテンツに対応するユーザコントロールデータのUC(0, S)が「0」で



あるか否かを判断し、コンテンツに対応するUC (0, S) が「0」であると判断された場合、このコンテンツはバス113上で保護すべきコンテンツであることになるので、ステップS196において、入出力制御部122は、相互認証部121を制御し、AVボード112との共通鍵を用いて、再生されたコンテンツを暗号化させ、バス113を介してAVボード112に出力させる。したがって、バス113上において不正なコピーが防止される。

#### 【0162】

ステップS195において、コンテンツに対応するUC (0, S) が「0」ではないと判断された場合（コンテンツに対応するUC (0, S) が「1」であると判断された場合）、このコンテンツは、バス113上で保護不要のコンテンツであるため、AVボード112からの保護すべきコンテンツの再生コマンドと矛盾するため、ドライブ111の再生処理は終了する。

#### 【0163】

一方、例えば、ユーザは、光ディスク141に記録されている保護不要のコンテンツを、HDD114に保存（記録）させるために、図示せぬ入力部などを介して、HDD114に、コンテンツの再生コマンドを入力する。HDD114は、バス113を介して、ドライブ111に再生コマンドを送信してくるので、ステップS191において、相互認証部121は、HDD114からの再生コマンドを入力する。

#### 【0164】

ステップS192において、入出力制御部122は、相互認証部121からの情報に基づいて、コンテンツを出力する機器（いまの場合、HDD114）が、相互認証されていないと判断する。このとき、ステップS197において、入出力制御部122は、HDD114からの再生コマンドが、保護すべきコンテンツの再生コマンドであるか否かを判断する。

#### 【0165】

ステップS193において、または、ステップS197において、コンテンツを出力する機器からの再生コマンドが、保護不要のコンテンツの再生コマンドであると判断された場合、ステップS198において、記録再生処理部123は、

光ディスク 141 から指示されたコンテンツを再生する。ステップ S199 において、入出力制御部 122 は、そのコンテンツに対応するユーザコントロールデータの UC (0, S) が「1」であるか否かを判断する。コンテンツに対応する UC (0, S) が「1」であると判断された場合、このコンテンツがバス 113 上で保護不要のコンテンツであることになるので、ステップ S200 において、入出力制御部 122 は、相互認証部 121 を制御し、再生されたコンテンツをそのまま（生データのまま）、バス 113 を介してコンテンツを出力する機器（いまの場合、AV ボード 112 または HDD 114）に出力させる。

#### 【0166】

また、ステップ S197 において、HDD 114 からのコマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、または、ステップ S199 において、コンテンツに対応する UC (0, S) が「1」ではないと判断された場合（コンテンツに対応する UC (0, S) が「0」であると判断された場合）、相互認証されていない HDD 114 へは、保護すべきコンテンツの出力はできないので、エラーとなり、ドライブ 111 の出力処理は、強制的に終了される。すなわち、ドライブ 111 においては、HDD 114 から保護すべきコンテンツの再生コマンドは拒否される。また、保護不要のコンテンツの再生コマンドであったとしても、実際にバス 113 上において、保護すべきコンテンツであった場合は、出力されない。

#### 【0167】

以上のようにして、相互認証されている AV ボード 112 への再生コマンドに対して、バス 113 上で保護すべきコンテンツは、共通鍵で暗号化され、バス 113 を介して、AV ボード 112 に出力され、バス 113 上で保護不要のコンテンツは、そのまま（暗号化させずに）、バス 113 を介して、AV ボード 112 に出力される。そして、後述する図 20 のステップ S201 において、AV ボード 112 の相互認証部 131 により受信される。

#### 【0168】

一方、相互認証されていない HDD 114 への再生コマンドに対しては、バス 113 上で保護すべきコンテンツは、出力されないが、バス 113 上で保護不要

のコンテンツは、そのまま（暗号化させずに）、バス 1 1 3 を介して、HDD 1 1 4 に出力される。これにより、HDD 1 1 4 において、保護不要のコンテンツが記憶できるので、ストレージ運用が可能になる。

#### 【0 1 6 9】

また、保護されるべきコンテンツは、ディスク ID および R K B を作用させたブロック鍵、およびコンテンツを送受信する装置間（いまの場合、ドライブ 1 1 1 および A V ボード 1 1 2）における相互認証されている共通鍵の両方で暗号化されているため、汎用的なバス 1 1 3 を介しても、不当なコピーを抑制することができる。

#### 【0 1 7 0】

なお、既存の記録再生装置において光ディスクに記録された保護すべきコンテンツに対応するユーザコントロールデータ 2 0 2（1 8 バイト）の先頭バイト U C（0, S）の最下位ビットには、もともと「0」が格納されている。したがって、既存のデータフォーマットにより記録した保護すべきコンテンツに対しても、上述した保護すべきコンテンツの再生処理が実行される（相互認証されている機器に対しては、共通鍵で暗号されて出力され、相互認証されていない機器に対しては、出力が禁止される）ので、汎用的なバス 1 1 3 を介しても、不当なコピーを抑制することができる。すなわち、既存のもののとの互換性が保たれる。

#### 【0 1 7 1】

以上のようなドライブ 1 1 1 のコンテンツ再生処理に対応する A V ボード 1 1 2 の再生処理を、図 2 0 のフローチャートを参照して説明する。

#### 【0 1 7 2】

ドライブ 1 1 1 は、A V ボード 1 1 2 からの保護すべきコンテンツの再生コマンドを受信し、光ディスク 1 4 1 よりコンテンツを再生し、バス 1 1 3 を介して出力してくるので、A V ボード 1 1 2 の相互認証部 1 3 1 は、ステップ S 2 0 1 において、そのコンテンツを受信し、ステップ S 2 0 2 において、受信したコンテンツが、ドライブ 1 1 1 の相互認証部 1 2 1 により暗号化されているか（保護すべきコンテンツであるか）否かを判断する。

#### 【0 1 7 3】

ステップ S 2 0 2 において、そのコンテンツが、共通鍵を用いて暗号化されており、保護すべきコンテンツであると判断された場合、ステップ S 2 0 3 において、相互認証部 1 3 1 は、ドライブ 1 1 1 との共通鍵を用いて、受信されたコンテンツを復号し、コンテンツ保護部 1 3 2 に出力する。すなわち、いま、このコンテンツは、ディスク I D および R K B を作用させたブロック鍵のみにより暗号化されている状態である。

#### 【0174】

ステップ S 2 0 4 において、コンテンツ保護部 1 3 2 は、ブロック鍵の生成処理を実行する。なお、このブロック鍵の生成処理は、図 1 6 を参照して説明したブロック鍵生成処理と同様であるので、その説明は繰り返しになるので、省略するが、ステップ S 2 0 4 において、光ディスク 1 4 1 の R K B を作用させたディスク鍵が取得され、取得されたディスク鍵および光ディスク 1 4 1 のディスク I D が生成されるので、ステップ S 2 0 5 において、暗号化部 2 5 4 は、相互認証部 1 3 1 からのコンテンツを、ブロック鍵を用いて復号し、A V コンテンツ処理部 1 3 3 に供給する。

#### 【0175】

一方、ステップ S 2 0 2 において、受信したコンテンツが、暗号化されておらず、保護不要のコンテンツであると判断された場合、このコンテンツは復号する必要はない。したがって、相互認証部 1 3 1 およびコンテンツ保護部 1 3 2 を素通りするため、ステップ S 2 0 3 乃至 S 2 0 5 の処理はスキップされる。

#### 【0176】

ステップ S 2 0 6 において、A V コンテンツ処理部 1 3 3 は、コンテンツ保護部 1 3 2 から供給されたコンテンツを、例えば、MPEG (Moving Picture Experts Group) 方式でデコードし、再生する。ステップ S 2 0 7 において、出力部 1 3 5 は、再生されたコンテンツを出力する。

#### 【0177】

以上のようにして、ドライブ 1 1 1 と相互認証されている A V ボード 1 1 2 においては、光ディスク 1 4 1 に記録されている保護すべきコンテンツおよび保護不要のコンテンツの両方を出力することができる。

## 【0178】

なお、上記説明においては、AVボード112は、記録時および再生時に、保護すべきコンテンツであると判断してからブロック鍵を生成するように説明したが、このブロック鍵の生成処理は、光ディスク141が装着されるごとにAVボード112の保護コンテンツ部132において実行されるようにしてもよい。

## 【0179】

図21は、本発明の記録再生装置の他の構成例を示している。なお、図21の記録再生装置301の基本的な構成は、図4の記録再生装置101と同様であるが、図21の記録再生装置301においては、図4の記録再生装置101におけるドライブ111の相互認証部121が除かれている。

## 【0180】

したがって、図21の記録再生装置301においては、AVボード112は、バス113上に接続されていても、ドライブ111が、相互認証機能を有しないため、AVボード112において相互認証されず（共通鍵が共有されず）、AVボード112からのコンテンツの再生要求処理は実行されないが、相互認証機能を有しないHDD114との保護不要のコンテンツの送受信処理が実行される。

## 【0181】

この記録再生装置301のドライブ111の記録処理を、図22のフローチャートを参照して説明する。なお、図22のステップS211乃至S214は、図18のステップS161およびステップS166乃至S168と同様の処理であり、その詳細な説明は繰り返しになるので省略する。

## 【0182】

したがって、ステップS211において、HDD114からの保護不要のコンテンツが、バス113を介して記録再生処理部123に受信され、ステップS212において、入出力制御部122により、相互認証部121に入力されたコンテンツが共通鍵で暗号化されていないので、いまの記録コマンドが、バス113上で保護すべきコンテンツの記録コマンドではないと判断される。ステップS213において、記録再生処理部123により、コンテンツに対応するユーザコントロールデータのUC(0, S)に、バス113上で保護不要のコンテンツであ

るという保護情報「1」が生成、格納され、ステップ S 2 1 4 において、記録再生処理部 1 2 3 により、この HDD 1 1 4 からの保護不要のコンテンツが光ディスク 1 4 1 に記録される。

#### 【0 1 8 3】

また、ステップ S 2 1 2 において、共通鍵で暗号化されているコンテンツが入力され、いまの記録コマンドが、保護すべきコンテンツの記録コマンドであると判断された場合、エラーとなり、ドライブ 1 1 1 の記録処理は、強制的に終了される。

#### 【0 1 8 4】

以上のようにして、相互認証機能を有さない HDD 1 1 4 からのバス 1 1 3 上で保護不要の保護情報とともに、コンテンツが光ディスク 1 4 1 に記録される。

#### 【0 1 8 5】

次に、この記録再生装置 3 0 1 のドライブ 1 1 1 の再生処理を、図 2 3 のフローチャートを参照して説明する。なお、図 2 3 のステップ S 2 2 1 乃至 S 2 2 5 の処理は、図 1 9 のステップ S 1 9 1 およびステップ S 1 9 7 乃至 S 2 0 0 の処理と同様の処理であり、その詳細な説明は繰り返しになるので省略する。

#### 【0 1 8 6】

したがって、例えば、ユーザは、光ディスク 1 4 1 に記録されている保護不要のコンテンツを、HDD 1 1 4 に保存（記録）させるために、入力部 6 1 7 を介して、HDD 1 1 4 へのコンテンツの再生コマンドを入力する。HDD 1 1 4 は、バス 1 1 3 を介して、ドライブ 1 1 1 に再生コマンドを送信してくるので、ステップ S 2 2 1 において、HDD 1 1 4 からの再生コマンドが入力され、ステップ S 2 2 2 において、入出力制御部 1 2 2 により、HDD 1 1 4 からの再生コマンドが、保護不要のコンテンツの再生コマンドであると判断された場合、ステップ S 2 2 3 において、記録再生処理部 1 2 3 により、指示されたコンテンツが光ディスク 1 4 1 から再生される。

#### 【0 1 8 7】

ステップ S 2 2 4 において、入出力制御部 1 2 2 により、そのコンテンツに対応するユーザコントロールデータの UC ( 0 , S ) が「1」であると判断された

場合、バス113上で保護不要のコンテンツであるとされ、ステップS225において、記録再生処理部123により再生されたコンテンツがそのまま（生データのまま）、バス113を介してHDD114に出力される。

#### 【0188】

一方、ステップS222において、HDD114からのコマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、または、ステップS224において、コンテンツに対応するUC(0, S)が「1」ではないと判断された場合、相互認証されていないHDD114へは、バス113上において保護すべきコンテンツの出力はできないので、エラーとなり、ドライブ111の記録処理は、強制的に終了される。

#### 【0189】

以上のようにして、HDD114への再生出力コマンドに対して、保護情報「1」が再生された場合、再生された、バス113上での保護不要のコンテンツは、そのまま（暗号化させずに）、バス113を介して、HDD14に出力される。したがって、保護不要のコンテンツは、共通鍵により暗号化もされていないので、HDD14に供給され、記憶されるようにできる。これにより、HDD14において、ストレージ運用が可能になる。

#### 【0190】

図24は、本発明を適用したさらに他の記録再生装置の構成例を示している。図24の記録再生装置401は、図4の記録再生装置101と基本的に同様な構成とされるが、図24のAVボード112においては、図4のAVボード112のコンテンツ保護部132が除かれており、代わりに、ドライブ111にコンテンツ保護部411が配置されている構成になっている。

#### 【0191】

したがって、図24のAVボード112においては、AVコンテンツ処理部133から供給されるコンテンツは、相互認証部131に出力される。相互認証部131より出力されるコンテンツは、AVコンテンツ処理部133に供給される。

#### 【0192】

また、図24のドライブ111においては、相互認証部121に入力されたコンテンツは、コンテンツ保護部411に供給される。コンテンツ保護部411の基本的な構成は、図4のコンテンツ保護部132と同様である。したがって、コンテンツ保護部411は、相互認証部121から供給されたコンテンツを、入出力制御部122の制御のもと、光ディスク141のディスクIDおよびRKB（ディスク鍵）を作用させたブロック鍵、または、RKB（ディスク鍵）のみを作用させたブロック鍵により暗号化し、記録再生処理部123に出力する。

#### 【0193】

記録再生処理部123は、光ディスク141から再生されたコンテンツを、コンテンツ保護部411に供給する。コンテンツ保護部411は、入出力制御部122の制御のもと、光ディスク141のディスクIDおよびRKBを作用させたブロック鍵、または、RKBのみを作用させたブロック鍵により復号し、相互認証部121に出力する。

#### 【0194】

図25は、図24のコンテンツ保護部411の構成を示している。なお、図24のコンテンツ保護部411は、図9のコンテンツ保護部132と基本的に同様の構成を有している。したがって、例えば、入出力制御部122により、AVボード112からの入力されたコンテンツが保護すべきコンテンツである（入力されたコンテンツの記録コマンドが、保護すべきコンテンツの記録コマンドである）と判断された場合、暗号化部254は、ディスク鍵、ディスクIDおよび記録情報を作用させて生成された、保護すべきコンテンツ用のブロック鍵を用いて、コンテンツを暗号化する。

#### 【0195】

また、入出力制御部122によりAVボード112からの入力されたコンテンツが保護不要のコンテンツである（入力されたコンテンツの記録コマンドが、保護不要のコンテンツの記録コマンドである）と判断された場合、暗号化部254は、少なくともRKBにより作成されたディスク鍵を作用させて生成された、保護不要のコンテンツ用のブロック鍵を用いて、コンテンツを暗号化する。RKBにより作成されたディスク鍵を作用させるのは、不正なドライブを排除するよう



にするためである。なお、これらの保護すべきコンテンツ用および保護不要のコンテンツ用のブロック鍵は、ドライブ 111 に光ディスク 141 が新しく装着される毎に、図 26 を参照して後述するブロック鍵生成処理により予め作成され、暗号化部 254 に内蔵されるメモリ（図示せず）に記憶されている。

#### 【0196】

次に、図 26 のフローチャートを参照して、図 24 のコンテンツ保護部 411 のブロック鍵生成処理を説明する。

#### 【0197】

ステップ S241 において、記録再生処理部 123 は、ドライブ 111 に新しく光ディスク 141 が装着されるまで待機しており、ステップ S241 において、光ディスク 141 が装着されたと判断した場合、ステップ S242 において、記録再生処理部 123 は、光ディスク 141 に記録されているディスク ID および RKB（ディスク情報）を再生し、コンテンツ保護部 411 に供給する。

#### 【0198】

ステップ S243 において、RKB 処理部 252 は、供給された RKB と内蔵するメモリに予め記憶されているデバイス ID およびデバイスキーを用いて、ディスク鍵を取得する。なお、この処理は、図 16 のステップ S123 の処理と同様であるため、その説明は繰り返しのになるので省略する。

#### 【0199】

ステップ S244 において、鍵生成部 253 は、記録再生処理部 123 より供給されたディスク ID、ステップ S243 において生成されたディスク鍵、および、コンテンツ保護部 411 の記録情報などを作用させて、保護すべきコンテンツ用のブロック鍵を生成し、暗号化部 254 に内蔵されるメモリなどに記憶する。

#### 【0200】

ステップ S245 において、鍵生成部 253 は、少なくとも、ステップ S243 において生成されたディスク鍵を作用させて、保護不要のコンテンツ用のブロック鍵を生成し、暗号化部 254 に内蔵されるメモリなどに記憶する。

#### 【0201】

以上のように、図 24 のコンテンツ保護部 411 においては、光ディスク 141 が装着されるたびに、保護すべきコンテンツ用および保護不要のコンテンツ用の 2 種類のブロック鍵が生成され、記憶される。なお、上記説明においては、ブロック鍵を生成したが、ブロック鍵を生成するためのディスク ID、ディスク鍵などを記憶しておき、暗号化する際に、そのコンテンツの保護状態に応じて、ブロック鍵を生成するようにしてもよい。

#### 【0202】

次に、図 27 のフローチャートを参照して、図 24 の AV ボード 112 の記録要求処理を説明する。なお、図 27 の記録要求処理は、図 15 の記録要求処理のステップ S103 および S104 が省略されている点を除き、図 15 の記録要求処理を同様の処理である。

#### 【0203】

したがって、ドライブ 111 においては、相互認証され、共通鍵が、AV ボード 112 と共有されている状態において、それ以降の処理が実行される。

#### 【0204】

ステップ S261 において、AV コンテンツ処理部 133 によりコンテンツが入力され、ステップ S262 において、AV コンテンツ処理部 133 により保護すべきコンテンツであると判断された場合、ステップ S263 において、そのコンテンツが、相互認証部 131 により、ドライブ 111 との共通鍵を用いて暗号化され、ステップ S264 において、ドライブ 111 に出力される。ステップ S262 において、保護不要のコンテンツであると判断されると、暗号化せず（ステップ S263 の処理はスキップされ）、ステップ S264 において、ドライブ 111 に出力される。

#### 【0205】

以上のようにして、AV ボード 112 からは、保護すべきコンテンツがドライブ 111 との共通鍵を用いて暗号化され、出力される。また、保護不要のコンテンツは、そのまま出力される。これに対応して実行される図 24 のドライブ 111 の記録処理を、図 28 のフローチャートを参照して説明する。なお、図 28 のステップ S301 乃至 S304、ステップ S306 および S307、並びにステ

ップS309およびS310は、図18のステップS161乃至S168と同様の処理であるため、その詳細な説明は省略する。

#### 【0206】

ステップS301において、ドライブ111の相互認証部121は、バス113を介して、AVボード112よりコンテンツを受信する。

#### 【0207】

ステップS302において、入出力制御部122は、相互認証部121からの情報に基づいて、このコンテンツを入力してきたAVボード112が、ドライブ111において相互認証されているか否かを判断し、AVボード112が、ドライブ111において相互認証されていると判断された場合、ステップS303において、入出力制御部122は、相互認証部121に入力されたコンテンツが共通鍵により暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス113上で保護すべきコンテンツの記録コマンドであるかを判断する。

#### 【0208】

ステップS303において、入力されたコンテンツの記録コマンドが、バス113上で保護すべきコンテンツの記録コマンドであると判断された場合、ステップS304において入出力制御部122は、相互認証部121を制御し、受信したコンテンツを、AVボード112との共通鍵で復号させ、そのコンテンツをコンテンツ保護部411に供給させる。

#### 【0209】

ステップS305において、暗号化部254は、供給されたコンテンツを、保護すべきコンテンツ用のブロック鍵を用いて暗号化する。この保護すべきコンテンツ用のブロック鍵は、図26を参照して上述したように、暗号化部254のメモリ内に予め記憶されている。そして、入出力制御部122は、記録再生処理部123を制御し、ステップS306において、このコンテンツに対応するユーザコントロールデータのUC(0, S)に、バス113上で保護すべきコンテンツであるという保護情報「0」を生成、格納し、ステップS310において、保護すべきコンテンツ用のブロック鍵を用いて暗号化されたコンテンツとともに、光

ディスク 141 に記録させる。

【0210】

一方、例えば、例えば、相互認証部を有しない HDD 114 に記憶されているコンテンツが入力される。このとき、ステップ S 301 において、HDD 114 からのコンテンツが、バス 113 を介して相互認証部 121 に受信される。ステップ S 302 において、コンテンツを入力してきた装置がドライブ 111 において相互認証されていないと判断され、ステップ S 307 において、入出力制御部 122 により、相互認証部 121 に入力されたコンテンツが共通鍵で暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス 113 上で保護すべきコンテンツの記録コマンドであるか否かが判断される。

【0211】

ステップ S 303 において、または、ステップ S 307 において、入力されたコンテンツの記録コマンドが、バス 113 上で保護不要のコンテンツの記録コマンドであると判断された場合、ステップ S 308 において、暗号化部 254 は、相互認証部 121 より供給されたコンテンツを、保護不要のコンテンツ用のブロック鍵を用いて暗号化する。この保護不要のコンテンツ用のブロック鍵は、図 26 を参照して上述したように、暗号化部 254 のメモリ内に予め記憶されている。

【0212】

ステップ S 309 において、入出力制御部 122 は、記録再生処理部 123 を制御し、コンテンツに対応するユーザコントロールデータの UC (0, S) に、バス 113 上で保護不要のコンテンツであるという保護情報「1」を生成、格納させ、ステップ S 310 において、生成された保護情報を、コンテンツとともに、光ディスク 141 に記録させる。

【0213】

また、ステップ S 307 において、入力されたコンテンツの記録コマンドが、バス 113 上で保護すべきコンテンツの記録コマンドであると判断された場合、エラーとなり、ドライブ 111 の記録処理は、強制的に終了される。

【0214】

以上のようにして、相互認証されているAVボード112からの保護すべきコンテンツは、ディスクIDおよびRKBを作用させたブロック鍵で暗号化され、バス113上で保護すべきコンテンツであるという保護情報「0」とともに光ディスク141に記録される。また、相互認証されているAVボード112からの保護不要のコンテンツ、または、相互認証されていないHDD114からの保護不要のコンテンツは、RKBのみを作用させたブロック鍵で暗号化され、バス113上で保護不要のコンテンツであるという保護情報「1」とともに光ディスク141に記録される。さらに、相互認証されていないHDD114からの保護すべきコンテンツは、光ディスク141には、記録されない。

#### 【0215】

次に、図29のフローチャートを参照して、図24のドライブ111のコンテンツ再生処理について説明する。なお、図29のステップS321乃至S325、並びにステップS327乃至S330は、図19のステップS191乃至S200と同様の処理であるため、その詳細な説明は省略する。

#### 【0216】

ユーザは、光ディスク141に記録されている保護すべきコンテンツを、AVボード112の出力部135から出力させるために、入力部を介して、AVボード112に、コンテンツの再生コマンドを入力する。AVボード112の相互認証部131は、バス113を介して、ドライブ111に再生コマンドを送信してくるので、ステップS321において、相互認証部121は、AVボード112からの再生コマンドを入力する。ステップS322において、相互認証部121からの情報に基づいて、コンテンツを出力するAVボード112が、ドライブ111において相互認証されていると判断された場合、ステップS323において、入出力制御部122により、AVボード112からの再生コマンドが、保護すべきコンテンツの再生コマンドであるか否かが判断される。

#### 【0217】

ステップS323において、AVボード112からの再生コマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、ステップS324において、記録再生処理部123により、光ディスク141から指示されたコンテ

ツが再生される。ステップS325において、入出力制御部122により、そのコンテンツに対応するユーザコントロールデータのUC(0, S)が「0」であると判断された場合、再生されたコンテンツがバス113上で保護すべきコンテンツであるとし、ステップS326において、暗号化部254は、内蔵するメモリに記憶された保護すべきコンテンツ用のブロック鍵を用いて、再生されたコンテンツを復号する。ステップS327において、相互認証部121は、暗号化部254より供給されたコンテンツを、AVボード112との共通鍵を用いて暗号化し、バス113を介してAVボード112に出力する。

#### 【0218】

一方、例えば、ユーザは、光ディスク141に記録されている保護不要のコンテンツを、HDD114に保存(記録)させるために、入力部を介して、HDD114にコンテンツの再生コマンドを入力する。HDD114は、バス113を介して、ドライブ111に再生コマンドを送信してくるので、ステップS321において、相互認証部121は、HDD114からの再生コマンドを入力する。ステップS322において、相互認証部121からの情報に基づいて、コンテンツを出力するHDD114が、相互認証されていないと判断され、ステップS328において、HDD114からの再生コマンドが、保護すべきコンテンツの再生コマンドであるか否かが判断される。

#### 【0219】

ステップS323において、または、ステップS228において、HDD114からの再生コマンドが、保護不要のコンテンツの再生コマンドであると判断された場合、ステップS329において、記録再生処理部123により指示されたコンテンツが光ディスク141から再生され、ステップS330において、入出力制御部122は、そのコンテンツに対応するユーザコントロールデータのUC(0, S)が「1」であるか否かを判断する。ステップS230において、そのコンテンツに対応するユーザコントロールデータのUC(0, S)が「1」であると判断された場合、再生されたコンテンツがバス113上で保護不要のコンテンツであるとし、ステップS331において暗号化部254は、内蔵するメモリに記憶された保護不要のコンテンツ用のブロック鍵を用いて、復号し、コンテン

ッをそのまま（生データのまま）、相互認証部121およびバス113を介して、AVボード112またはHDD114に出力する。

#### 【0220】

また、ステップS325において、コンテンツに対応するUC(0, S)が「0」ではないと判断された場合、ステップS328において、HDD114からの再生コマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、または、ステップS330において、コンテンツに対応するUC(0, S)が「1」ではないと判断された場合、エラーとなり、ドライブ111の記録処理は、強制的に終了される。

#### 【0221】

以上のようにして、相互認証されているAVボード112からの再生コマンドに対して、バス113上で保護すべきコンテンツは、共通鍵で暗号化され、バス113を介して、AVボード112に出力され、バス113上で保護不要のコンテンツは、そのまま（暗号化させずに）、バス113を介して、AVボード112に出力される。そして、後述する図30のステップS361において、AVボード112の相互認証部131により受信される。

#### 【0222】

この図24のドライブ111のコンテンツ再生処理に対応するAVボード112の再生処理を、図30のフローチャートを参照して説明する。なお、図30の再生処理は、図20の再生処理のステップS204およびS205を省略した点を除き、図20の場合と同様である。

#### 【0223】

ステップS361において、相互認証部131により、ドライブ111からのコンテンツが受信され、ステップS362において、そのコンテンツが、共通鍵を用いて暗号化されており、保護すべきコンテンツであると判断された場合、ステップS363において、ドライブ111との共通鍵を用いて受信されたコンテンツが復号される。

#### 【0224】

一方、ステップS362において、暗号化されておらず、保護不要のコンテン

ツであると判断された場合、このコンテンツは、暗号化されていないので、復号する必要はない。したがって、相互認証部131およびコンテンツ保護部132を素通りするため、ステップS363の処理はスキップされる。

#### 【0225】

ステップS364において、AVコンテンツ処理部133は、コンテンツ保護部132から供給されたコンテンツを、例えば、MPEG方式でデコードし、再生する。ステップS365において、出力部135は、再生されたコンテンツを出力する。

#### 【0226】

以上のようにして、ドライブ111と相互認証されているAVボード112においては、光ディスク141に記録されているバス113上で保護すべきコンテンツ、および、バス113上で保護不要のコンテンツの両方を出力することができる。

#### 【0227】

図31は、本発明の記録再生装置の他の構成例を示している。なお、図31の記録再生装置501の基本的な構成は、図24の記録再生装置401と同様であるが、図31の記録再生装置501においては、図24の記録再生装置401におけるドライブ111の相互認証部121が除かれている。

#### 【0228】

したがって、図31の記録再生装置501においては、AVボード112は、バス113上に接続されていても、ドライブ111が、相互認証機能を有しないため、AVボード112において相互認証されず（共通鍵が共有されず）、AVボード112からのコンテンツの再生要求処理は実行されないが、相互認証機能を有しないHDD114との保護不要のコンテンツの送受信処理が実行される。

#### 【0229】

この記録再生装置501のドライブ111の記録処理を、図32のフローチャートを参照して説明する。なお、図32のステップS401乃至S405は、図28のステップS301およびステップS307乃至S310と同様の処理であり、その説明は繰り返しになるので適宜省略する。



**【0230】**

したがって、ステップS401において、HDD114からの保護不要のコンテンツが、バス113を介して記録再生処理部123に受信され、ステップS402において、入出力制御部122により、相互認証部121に入力されたコンテンツが共通鍵で暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス113上で保護すべきコンテンツの記録コマンドではないと判断される。ステップS403において、暗号化部254により、保護不要のコンテンツ用のブロック鍵を用いて、コンテンツが暗号化される。

**【0231】**

ステップS404において、記録再生処理部123により、コンテンツに対応するユーザコントロールデータのUC(0, S)に、バス113上で保護不要のコンテンツであるという保護情報「1」が生成、格納され、ステップS405において、HDD114からの保護不要のコンテンツとともに、光ディスク141に記録される。

**【0232】**

また、ステップS402において、共通鍵で暗号化されているコンテンツが入力され、入力されたコンテンツの記録コマンドが、バス113上で保護すべきコンテンツの記録コマンドであると判断された場合、エラーとなり、ドライブ111の記録処理は、強制的に終了される。なお、共通鍵ではなく別の方法で暗号化されているコンテンツであれば、バス113上で保護不要のコンテンツとして処理させることも可能である。

**【0233】**

以上のようにして、相互認証機能を有さないHDD114からのバス113上で保護不要のコンテンツが光ディスク141に記録される。

**【0234】**

次に、この記録再生装置501のドライブ111の再生処理を、図33のフローチャートを参照して説明する。なお、図33のステップS421乃至S425は、図29のステップS321およびステップS328乃至S331と同様の処理であるため、その詳細な説明を省略する。

## 【0235】

したがって、例えば、ユーザは、光ディスク141に記録されている保護不要のコンテンツを、HDD114に保存（記録）させるために、入力部を介して、HDD114に、保護不要のコンテンツの再生コマンドを入力する。HDD114は、バス113を介して、ドライブ111に再生コマンドを送信してくるので、ステップS421において、HDD114からの再生コマンドが入力され、ステップS422において、HDD114からの再生コマンドが、保護不要のコンテンツの再生コマンドであると判断された場合、ステップS423において、記録再生処理部123により、光ディスク141から指示されたコンテンツが再生される。

## 【0236】

ステップS424において、入出力制御部122により、そのコンテンツに対応するユーザコントロールデータのUC(0, S)が「1」とであると判断された場合、再生されたコンテンツがバス113上で保護不要のコンテンツであるとされ、ステップS425において、暗号化部254により、保護不要のコンテンツ用のブロック鍵を用いて、復号され、コンテンツが、そのまま（生データのまま）、相互認証部121およびバス113を介してコンテンツを出力するAVボード112またはHDD114に出力される。

## 【0237】

一方、ステップS422において、HDD114からのコマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、または、ステップS424において、コンテンツに対応するUC(0, S)が「1」ではないと判断された場合、相互認証されていないHDD114へは、保護すべきコンテンツの出力はできないので、エラーとなり、ドライブ111の記録処理は、強制的に終了される。

## 【0238】

以上のようにして、HDD114への再生コマンドに対して、保護情報「1」が再生され、再生された保護不要のコンテンツは、そのまま（暗号化させずに）、バス113を介して、HDD114に出力される。したがって、バス113上で

保護不要のコンテンツは、暗号化もされていないので、HDD 14 に供給され、記憶されるようにできる。

#### 【0239】

また、相互認証されないHDD 14からのコンテンツは、HDD 14により保護すべきコンテンツであると示されたとしても、ドライブ111においては、保護すべきコンテンツとしては認識されず、保護不要のコンテンツとしてであれば、扱うようにできる。以上のように、コピーフリーのコンテンツのみを扱う相互認証しないストレージ運用が可能になる。

#### 【0240】

なお、上記説明においては、記録媒体を、光ディスク141としたが、記録媒体は、光ディスク141だけでなく、光ディスク141以外のメモリーカード（登録商標）、その他の記録媒体とすることもできる。

#### 【0241】

上述した一連の処理は、ハードウェアにより実行させることもできるし、ソフトウェアにより実行させることもできる。この場合、例えば、図4の記録再生装置101、図21の記録再生装置301、図24の記録再生装置401および図31の記録再生装置501は、図34に示されるような記録再生装置601により構成される。

#### 【0242】

図31において、CPU (Central Processing Unit) 611は、ROM (Read Only Memory) 612に記憶されているプログラム、または、HDD 619からRAM (Random Access Memory) 613にロードされたプログラムに従って各種の処理を実行する。RAM 613にはまた、CPU 611が各種の処理を実行する上において必要なデータなどが適宜記憶される。

#### 【0243】

CPU 611、ROM 612、およびRAM 613は、バス614を介して相互に接続されている。このバス614にはまた、入出力インタフェース615も接続されている。

#### 【0244】

入出力インタフェース 615 には、コンテンツの入出力の制御を行う A V ボード 616、キーボード、マウスなどよりなる入力部 617、C R T (Cathode Ray Tube)、L C D (Liquid Crystal Display) などよりなるディスプレイ、並びにスピーカなどよりなる出力部 618、H D D 619、モデム、ターミナルアダプタなどより構成される通信部 620 が接続されている。通信部 620 は、バスや図示しないネットワークを介しての通信処理を行う。

#### 【0245】

入出力インタフェース 615 にはまた、必要に応じてドライブ 630 が接続され、磁気ディスク 631、光ディスク 632、光磁気ディスク 633、或いは半導体メモリ 634 などが適宜装着され、それから読み出されたコンピュータプログラムが、必要に応じて H D D 619 にインストールされる。

#### 【0246】

一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば、汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

#### 【0247】

この記録媒体は、図 34 に示すように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク 631 (フレキシブルディスクを含む)、光ディスク 632 (C D - R O M (Compact Disk-Read Only Memory)、D V D (Digital Versatile Disk) を含む)、光磁気ディスク 633 (M D (Mini-Disk) (商標) を含む)、もしくは半導体メモリ 634 などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されている R O M 612 や、H D D 619 などで構成される。

#### 【0248】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時

系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【 0 2 4 9 】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【 0 2 5 0 】

【発明の効果】

以上の如く、本発明によれば、保護の要不要に基づいて、コンテンツを柔軟に保護することができる。また、本発明によれば、コンテンツの不正コピーが抑制される。さらに、本発明によれば、P C ストレージ運用が可能になる。

【図面の簡単な説明】

【図 1】

従来の記録再生装置の構成例を示すブロック図である。

【図 2】

従来の記録再生装置の他の構成例を示すブロック図である。

【図 3】

従来の記録再生装置のさらに他の構成例を示すブロック図である。

【図 4】

本発明を適用した記録再生装置の構成例を示すブロック図である。

【図 5】

本発明のデータフォーマットの構成例を示す図である。

【図 6】

図 5 のデータフレームの構成例を示す図である。

【図 7】

図 5 のスクランブルデータフレームの構成例を示す図である。

【図 8】

図 5 のユーザコントロールデータの構成例を示す図である。

【図 9】

図 4 のコンテンツ保護部 1 3 2 の構成例を示すブロック図である。

**【図 10】**

本発明のディスク鍵について説明するツリー構造図である。

**【図 11】**

本発明のディスク鍵に使用される R K B の例を説明する図である。

**【図 12】**

図 11 の R K B の使用例を説明する図である。

**【図 13】**

図 4 の A V ボードの相互認証処理を説明するフローチャートである。

**【図 14】**

図 4 のドライブの相互認証処理を説明するフローチャートである。

**【図 15】**

図 4 の A V ボードの記録要求処理を説明するフローチャートである。

**【図 16】**

図 15 のステップ S 103 のブロック鍵生成処理を説明するフローチャートである。

**【図 17】**

図 16 の処理に対応する図 4 のドライブのディスク情報再生処理を説明するフローチャートである。

**【図 18】**

図 4 のドライブの記録処理を説明するフローチャートである。

**【図 19】**

図 4 のドライブの再生処理を説明するフローチャートである。

**【図 20】**

図 4 の A V ボードの再生処理を説明するフローチャートである。

**【図 21】**

図 4 の記録再生装置の他の構成例を示すブロック図である。

**【図 22】**

図 21 のドライブの記録処理を説明するフローチャートである。

**【図 23】**

図 21 のドライブの再生処理を説明するフローチャートである。

【図 24】

本発明の記録再生装置の他の構成例を示すブロック図である。

【図 25】

図 24 のコンテンツ保護部 411 の構成例を示すブロック図である。

【図 26】

図 24 のドライブのブロック鍵生成処理を説明するフローチャートである。

【図 27】

図 24 の AV ボードの記録要求処理を説明するフローチャートである。

【図 28】

図 24 のドライブの記録処理を説明するフローチャートである。

【図 29】

図 24 のドライブの再生処理を説明するフローチャートである。

【図 30】

図 24 の AV ボードの再生処理を説明するフローチャートである。

【図 31】

図 24 の記録再生装置の他の構成例を示すブロック図である。

【図 32】

図 31 のドライブの記録処理を説明するフローチャートである。

【図 33】

図 31 のドライブの再生処理を説明するフローチャートである。

【図 34】

本発明の記録再生装置の他の構成例を示すブロック図である。

【符号の説明】

101 記録再生装置, 111 ドライブ, 112 AV ボード, 113 バス, 114 HDD, 121 相互認証部, 122 入出力制御部, 123 記録再生処理部, 131 相互認証部, 132 コンテンツ処理部, 141 光ディスク, 202 ユーザコントロールデータ, 252 RKB 処理部, 253 鍵生成部, 254 暗号化部, 301 記録再生装置, 401 記録再生装置,

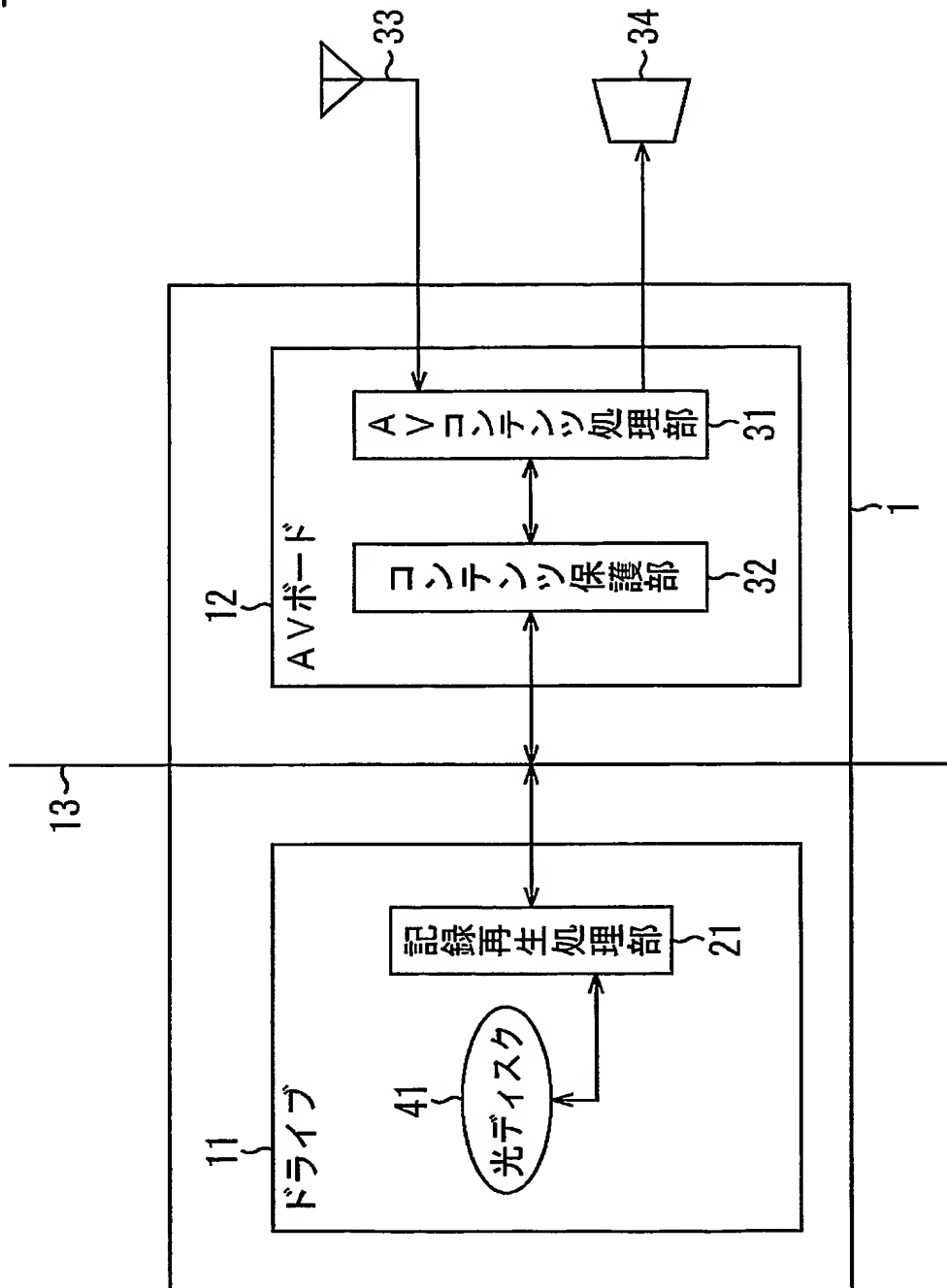
4 1 1 コンテンツ保護部, 5 0 1 記録再生装置



【書類名】 図面

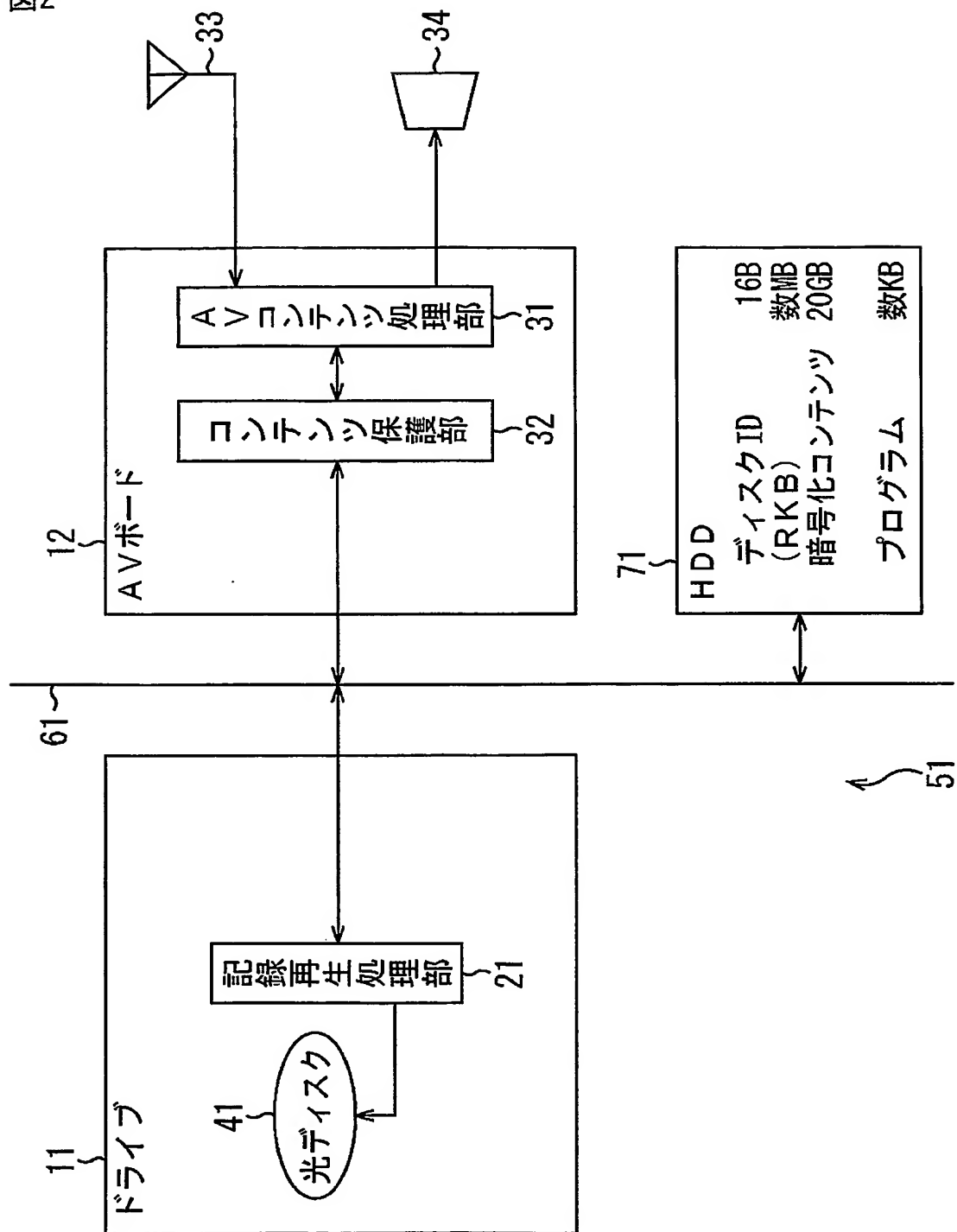
【図 1】

図1



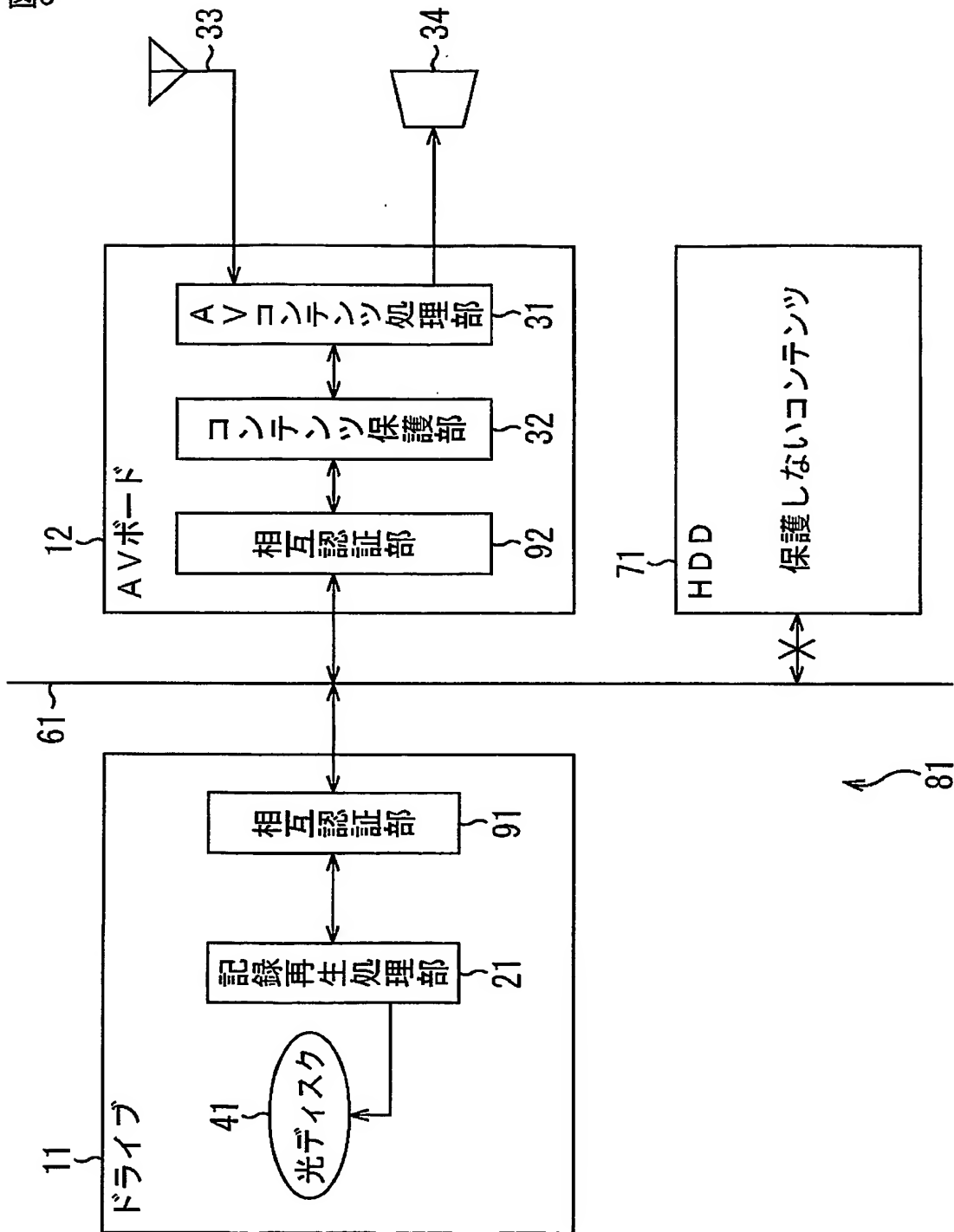
【図 2】

図2



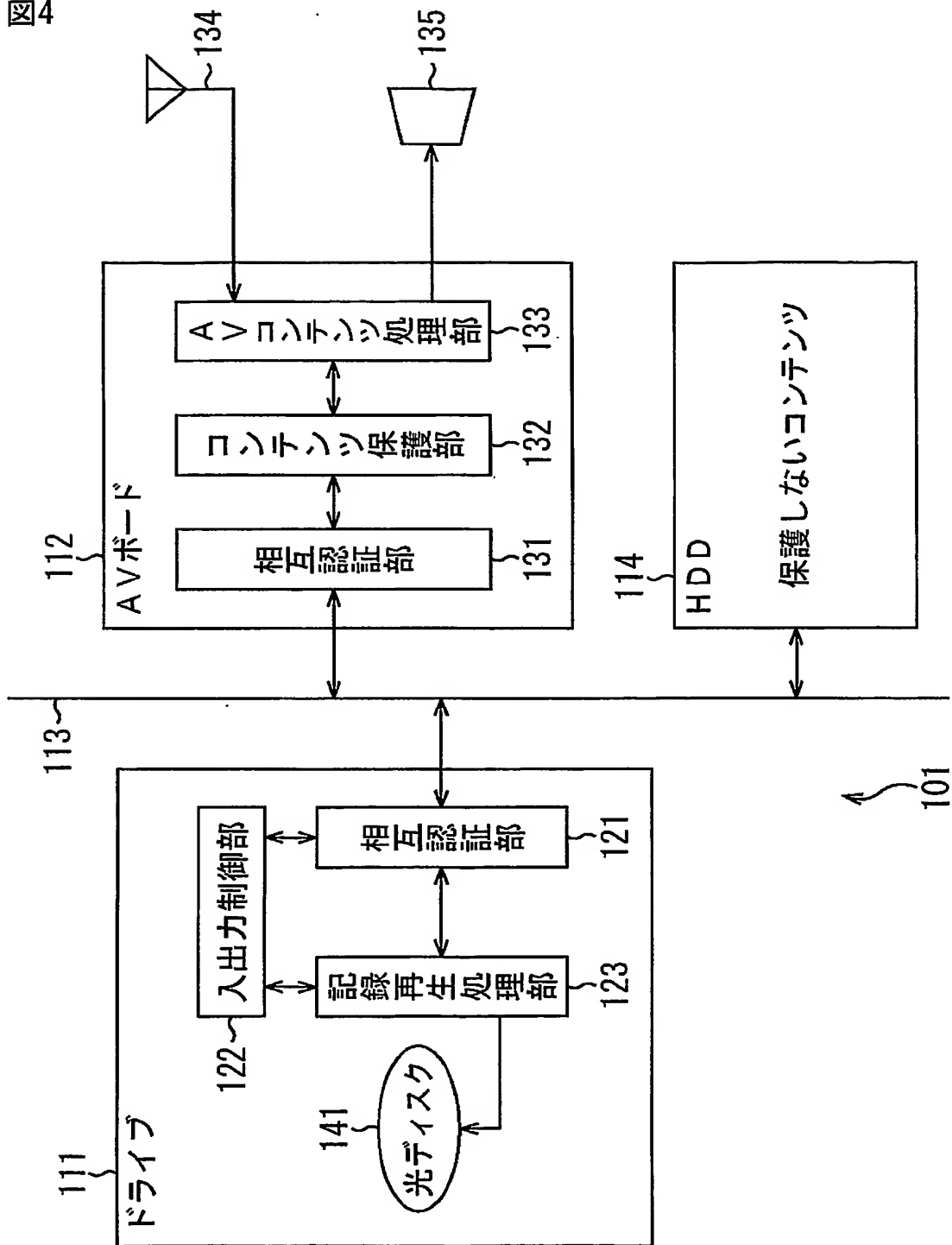
【図 3】

図3



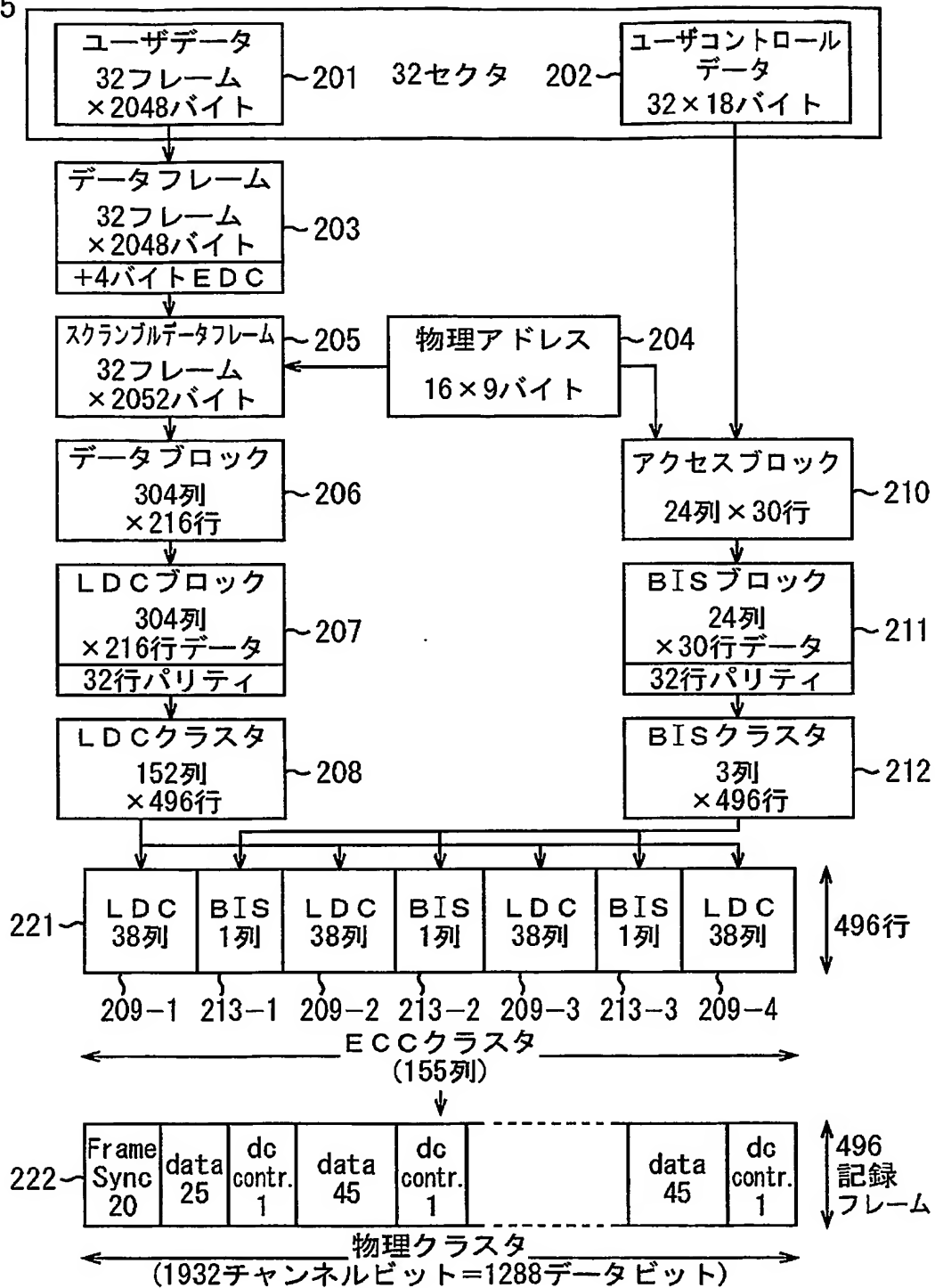
【図 4】

図4



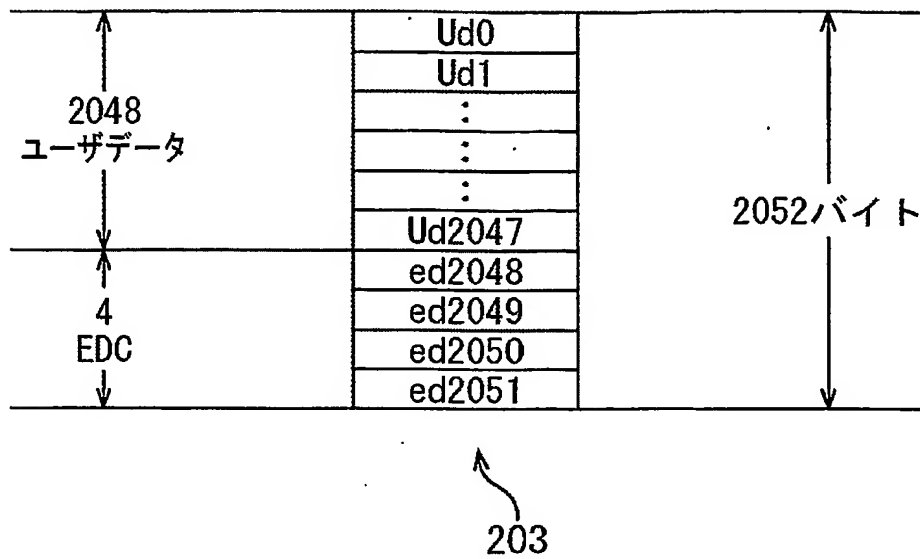
【図5】

図5



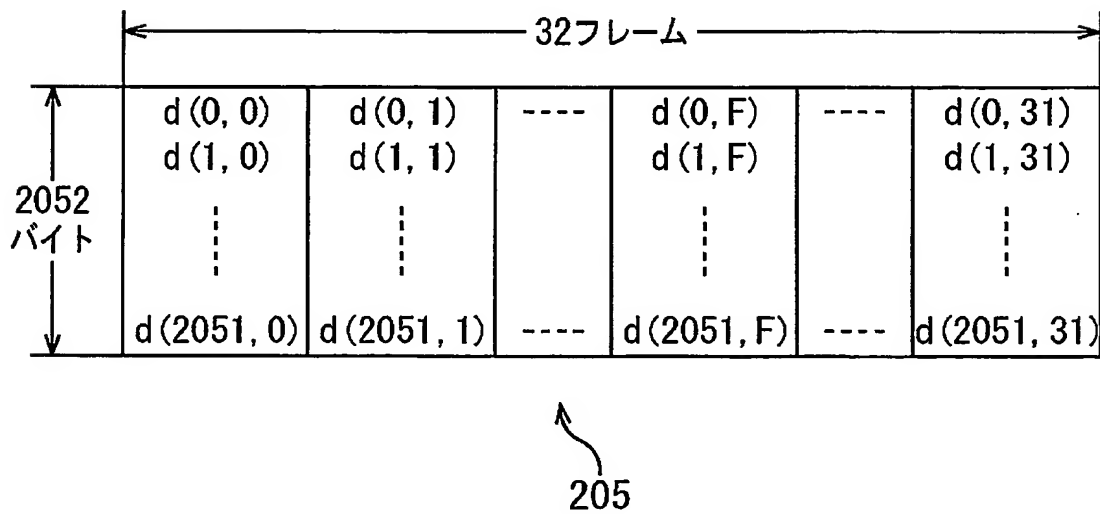
【図 6】

図6



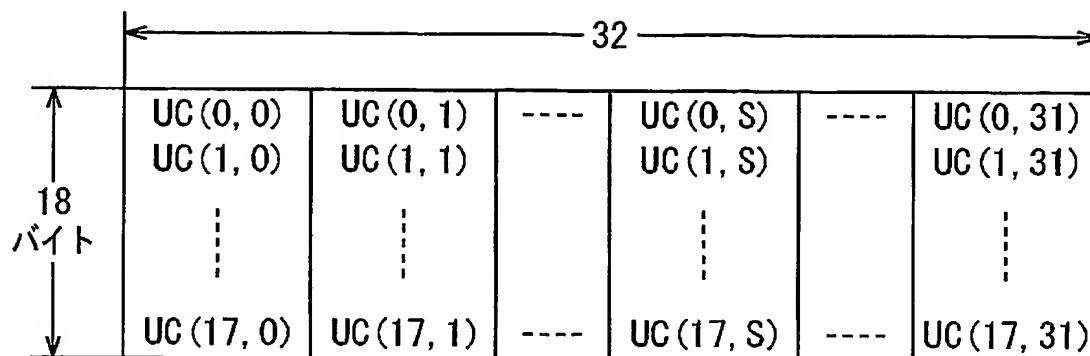
【図 7】

図7



【図 8】

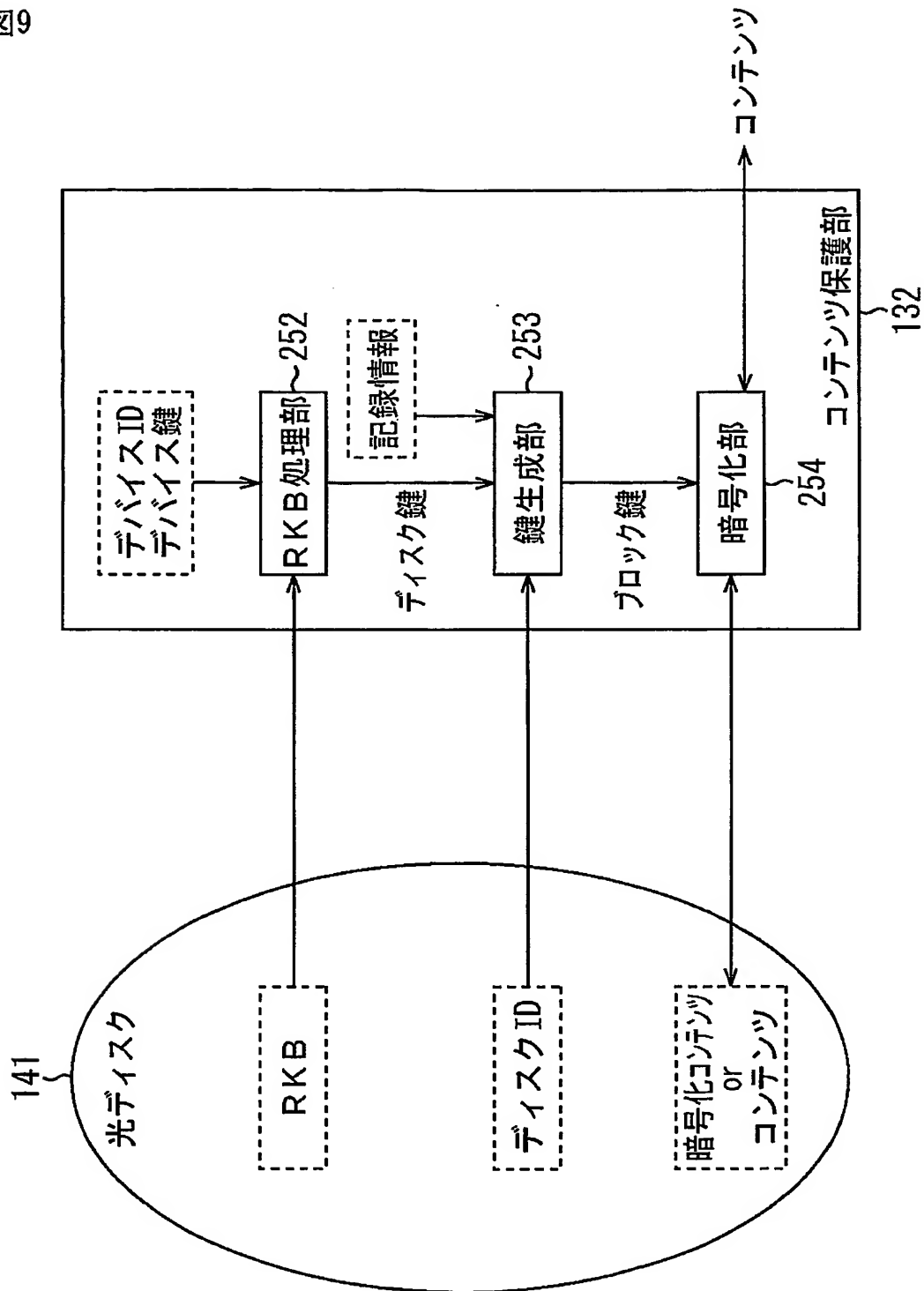
図8



202

【図 9】

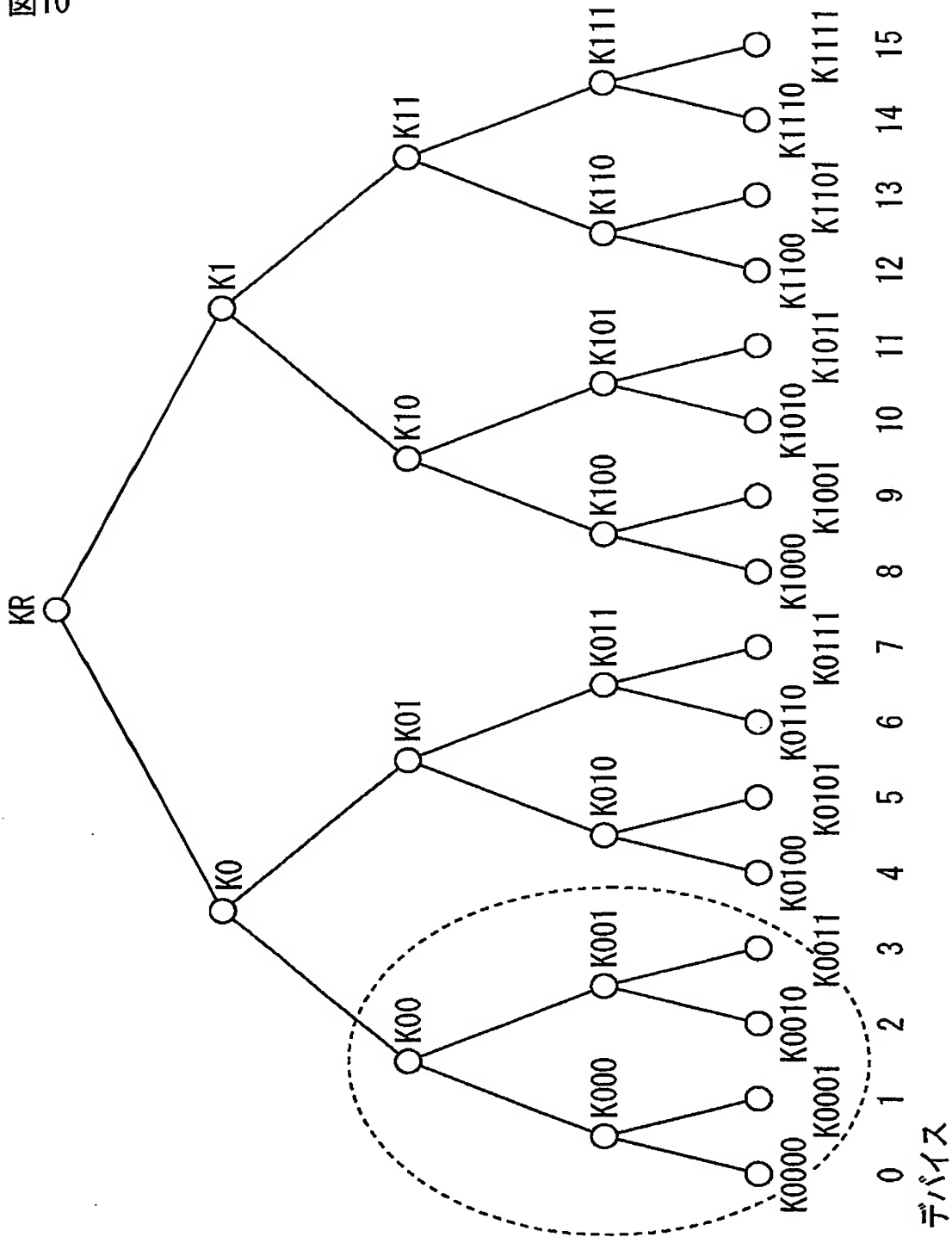
図9





【図 10】

図10



【図 11】

図11

A

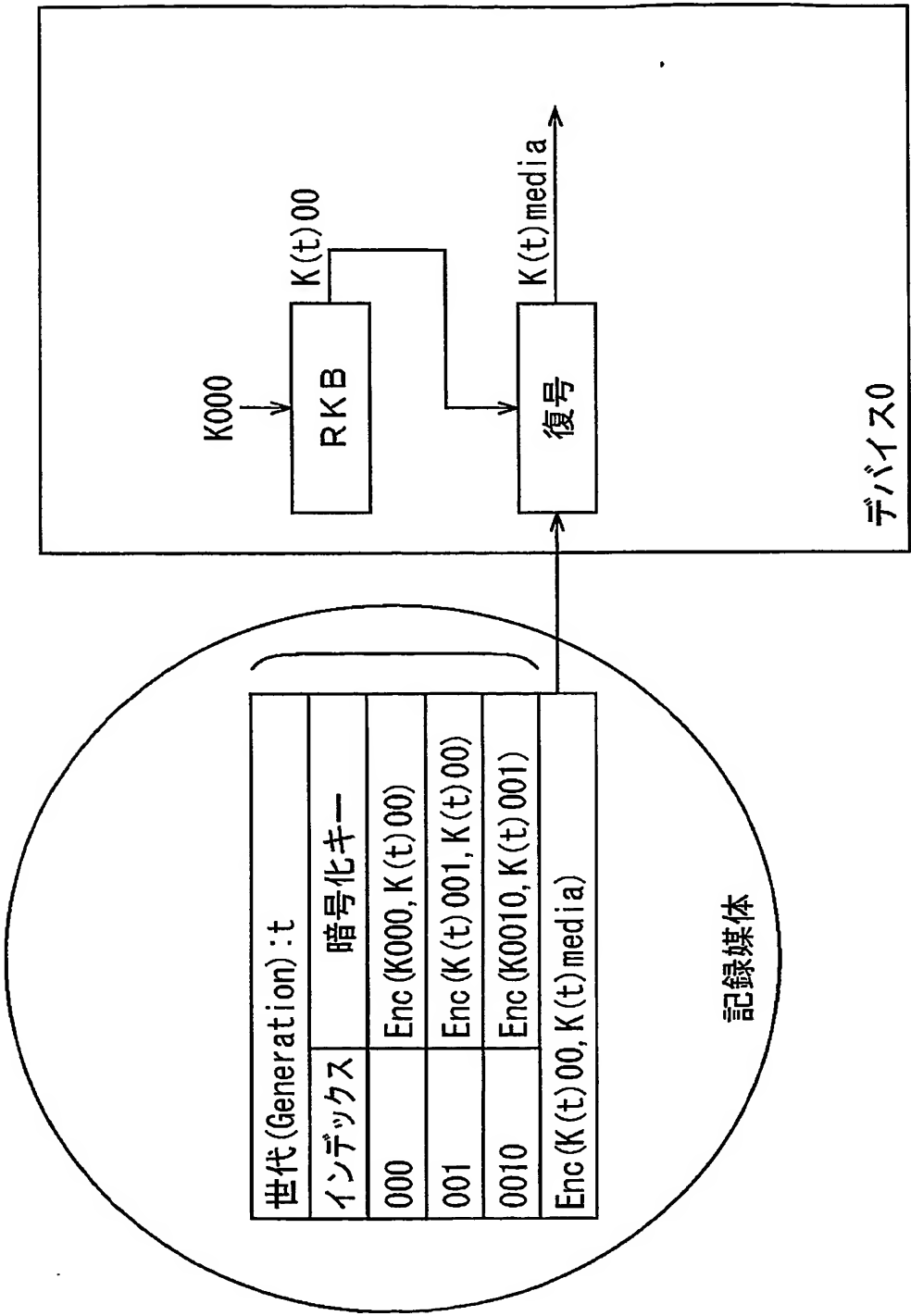
バージョン(Version):t	
インデックス	暗号化キー
0	Enc (K (t) 0, K (t) R)
00	Enc (K (t) 00, K (t) 0)
000	Enc (K000, K (t) 00)
001	Enc (K (t) 001, K (t) 00)
0010	Enc (K0010, K (t) 001)

B

バージョン(Version):t	
インデックス	暗号化キー
000	Enc (K000, K (t) 00)
001	Enc (K (t) 001, K (t) 00)
0010	Enc (K0010, K (t) 001)

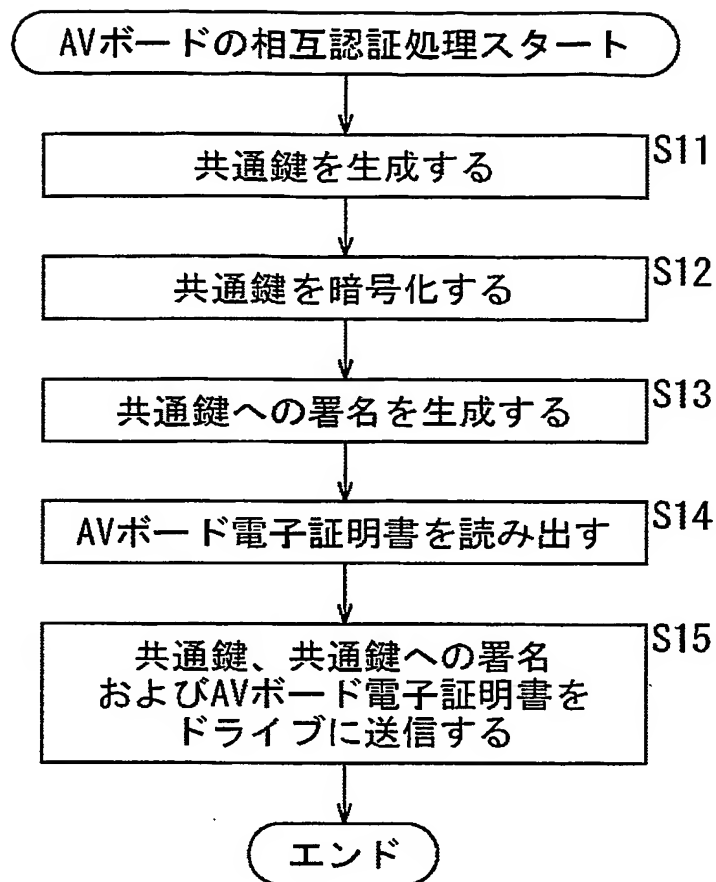
【図 12】

図12



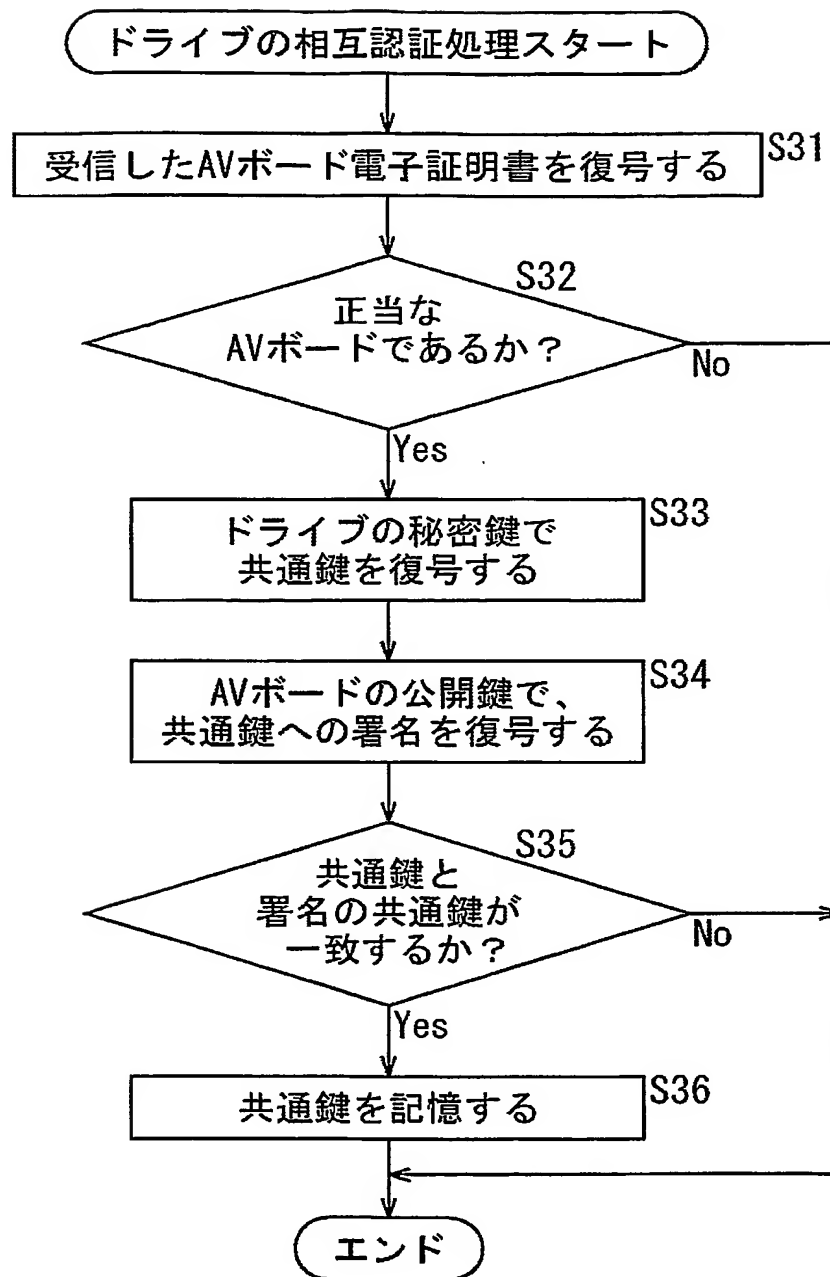
【図 13】

図13



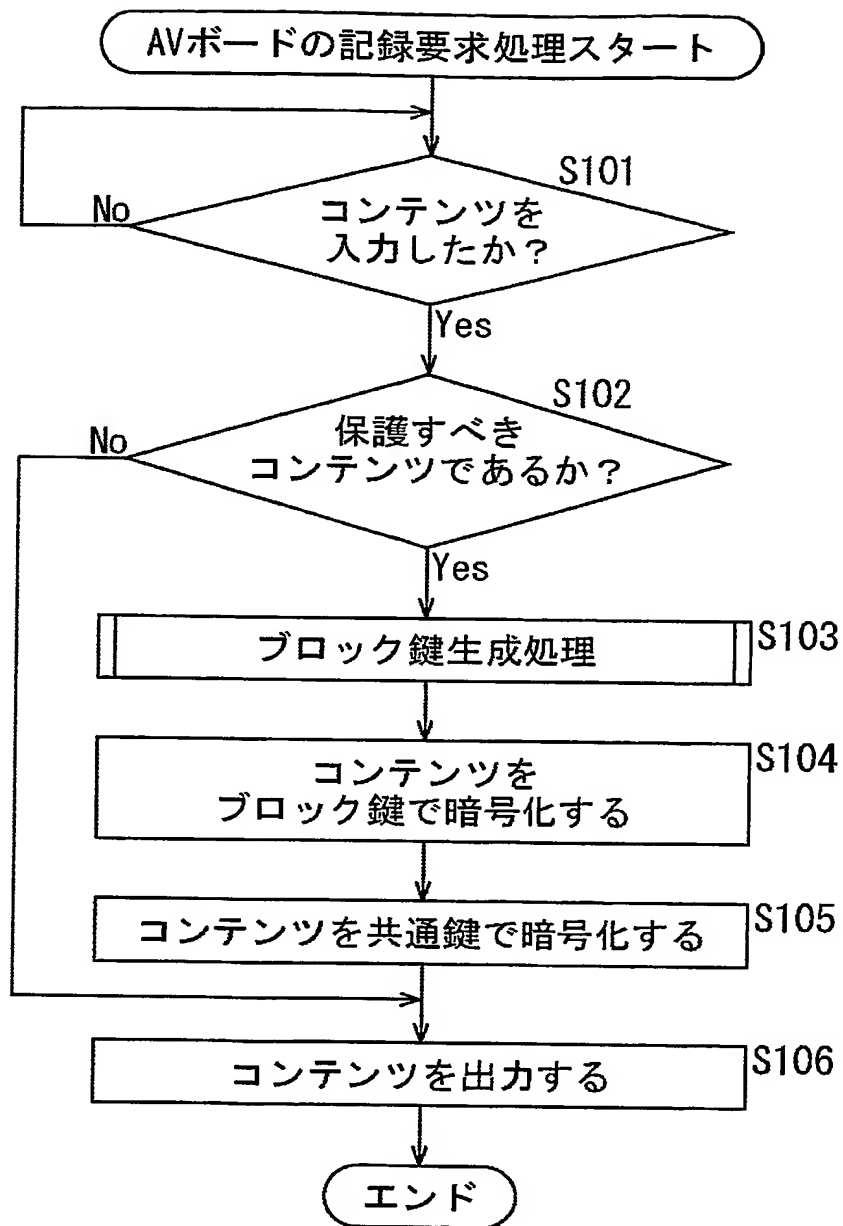
【図14】

図14



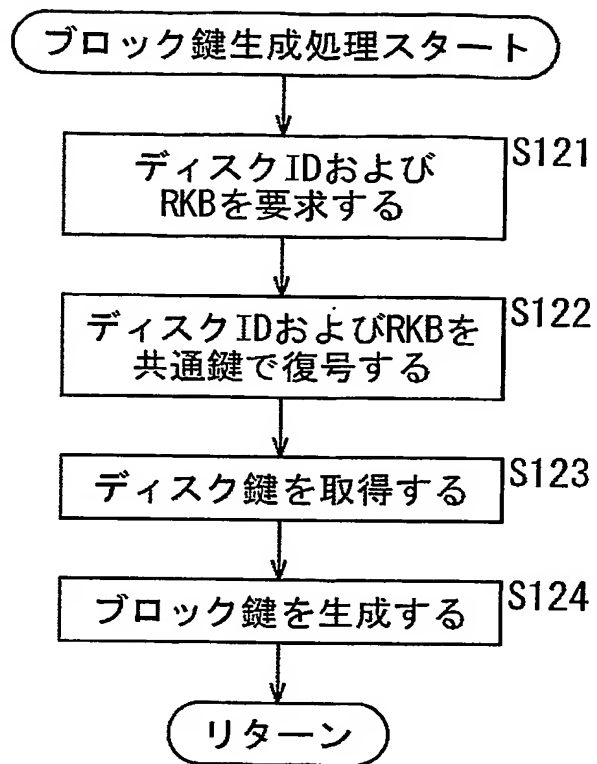
【図15】

図15



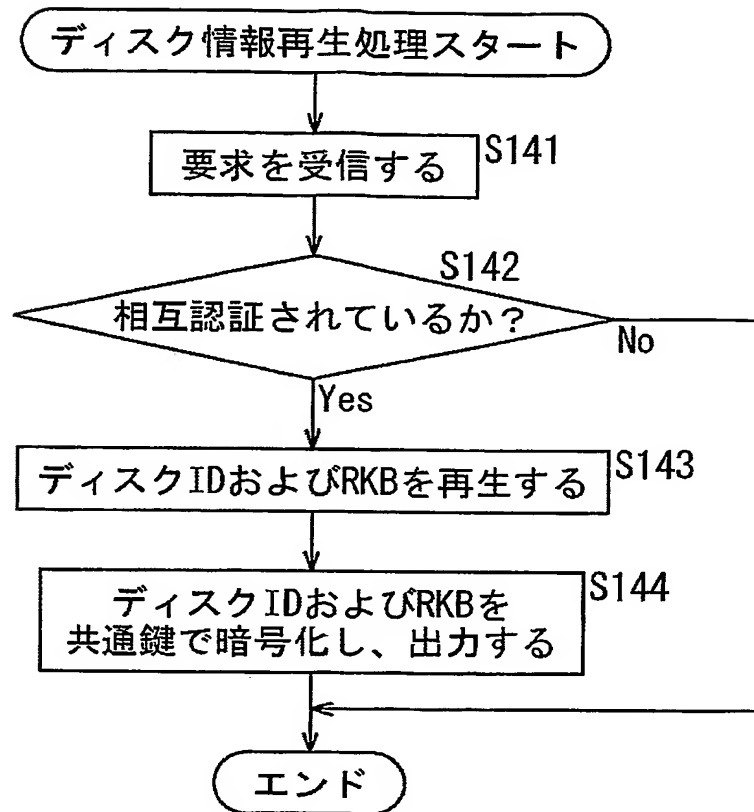
【図 16】

図16



【図 17】

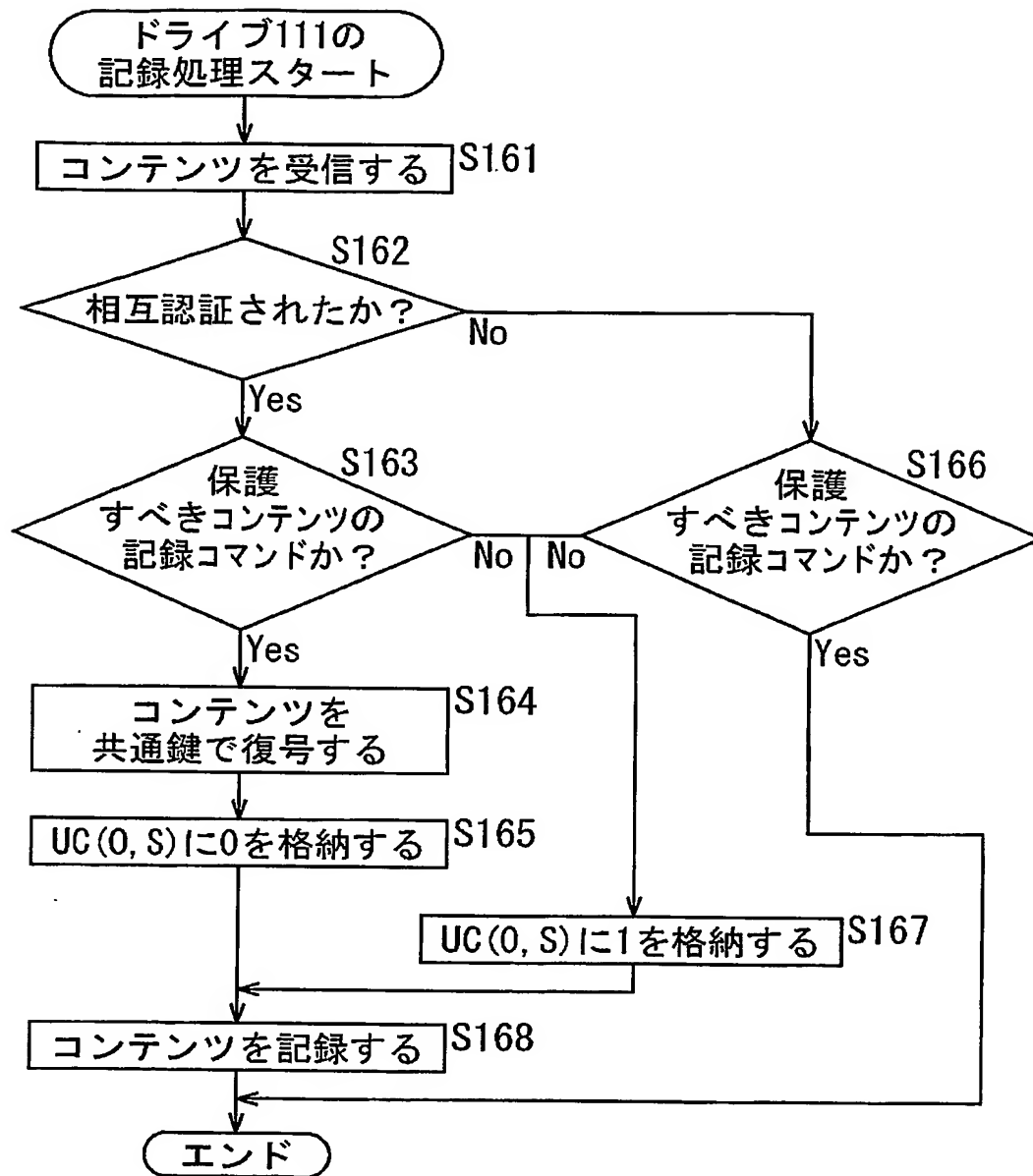
図17





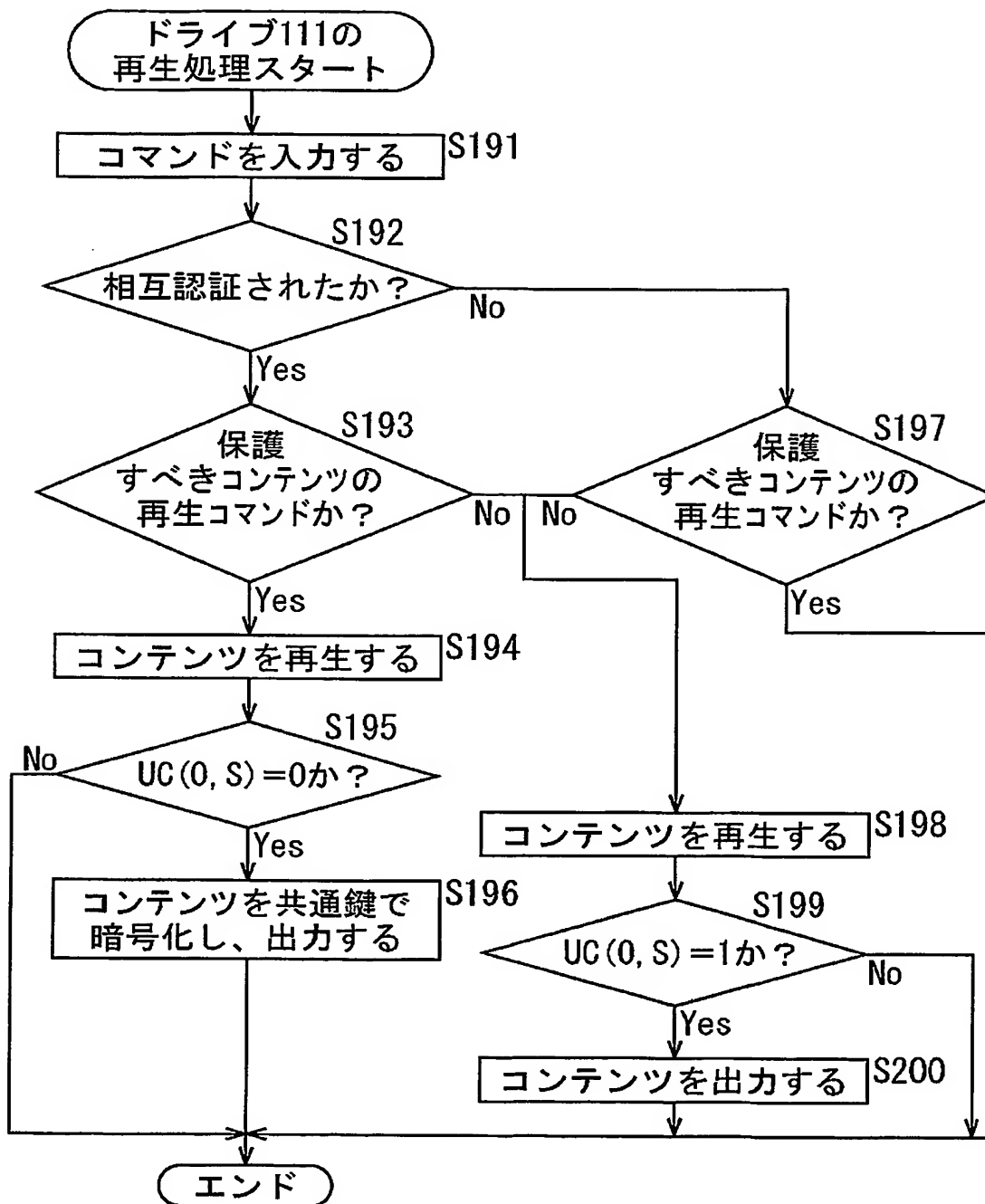
【図18】

図18



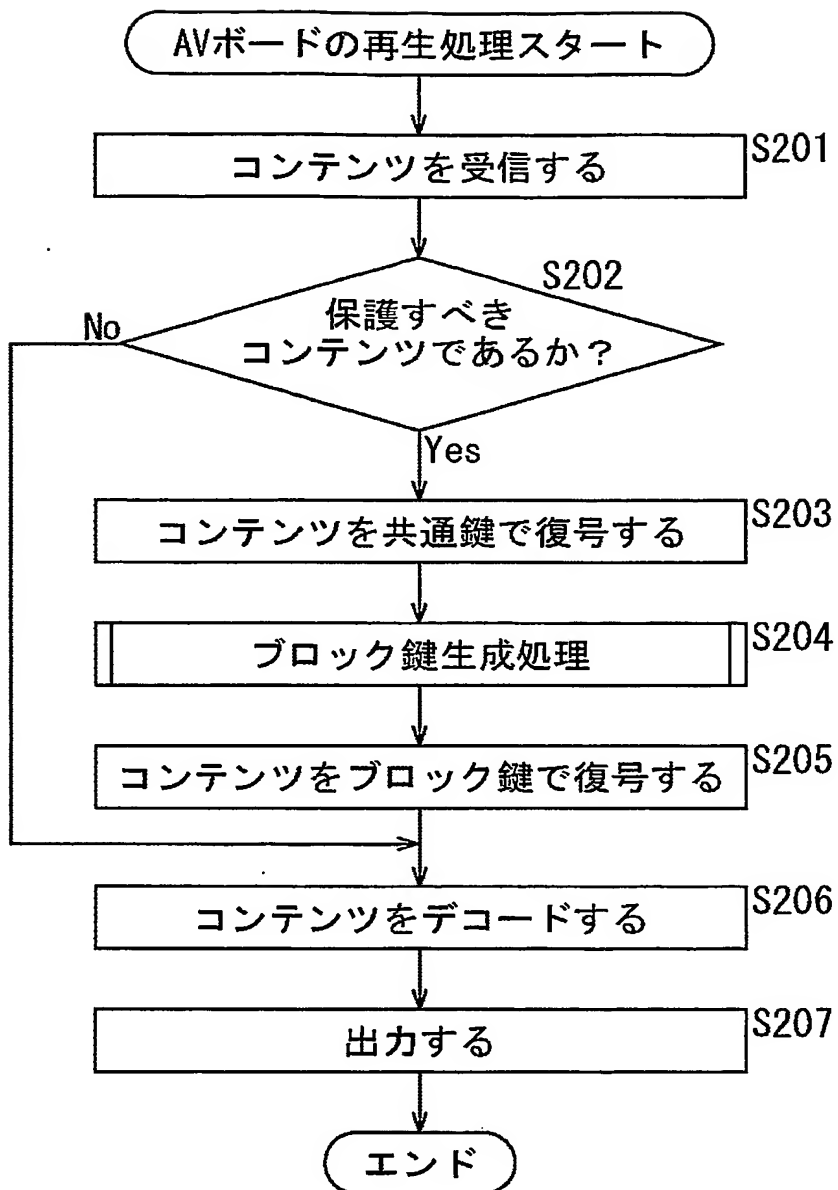
【図 19】

図19



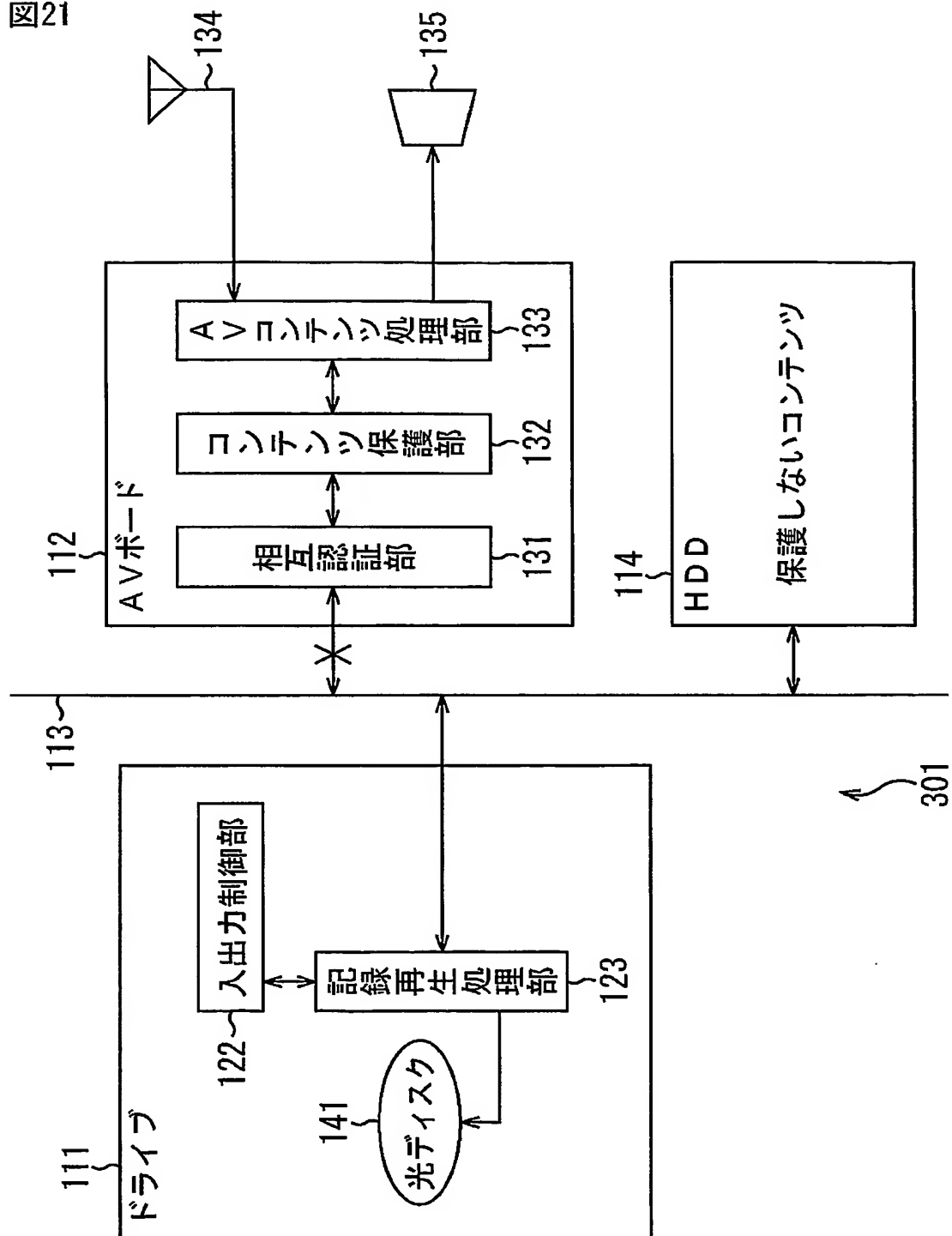
【図 20】

図20



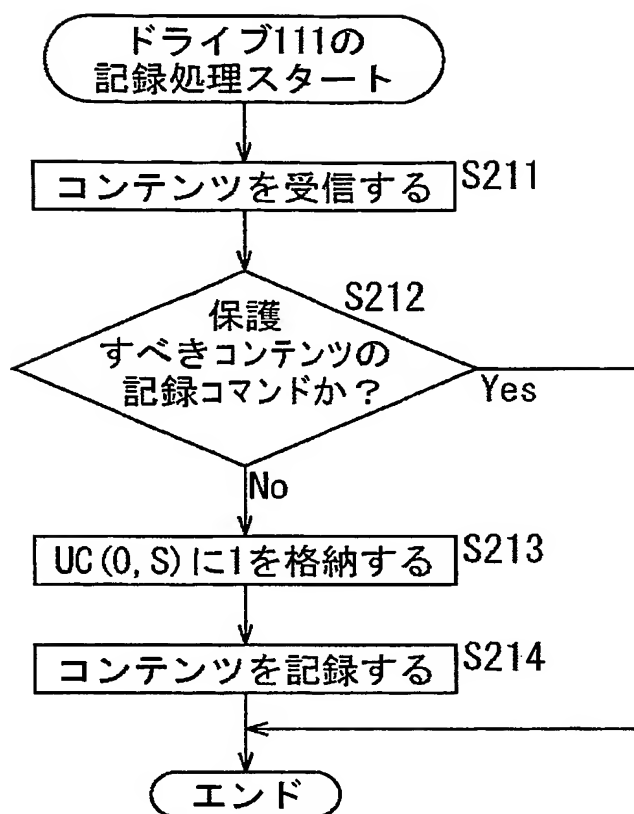
【図 21】

図21



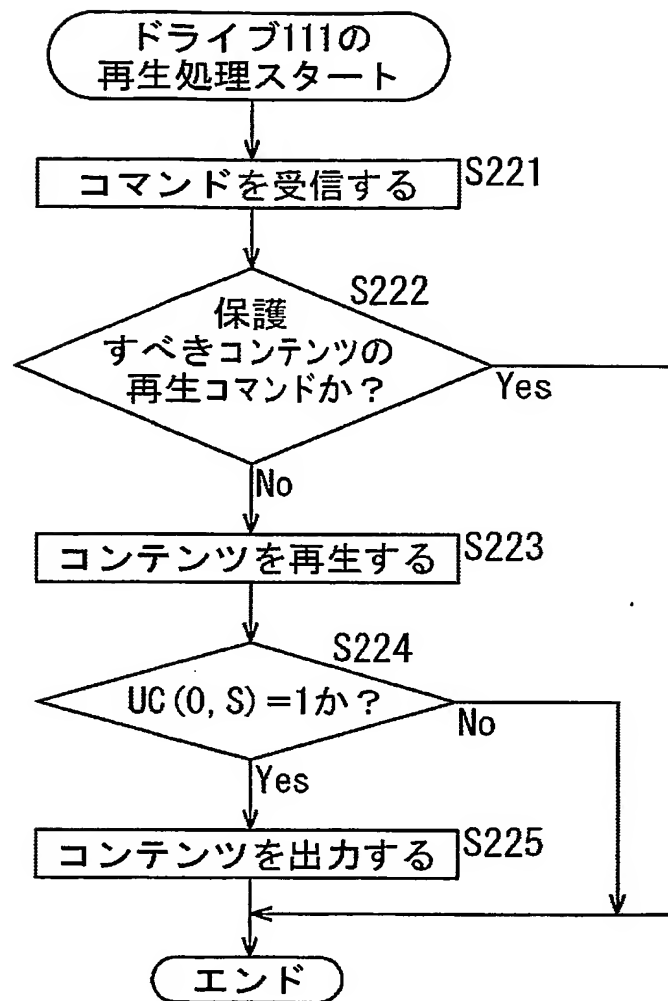
【図 22】

図22



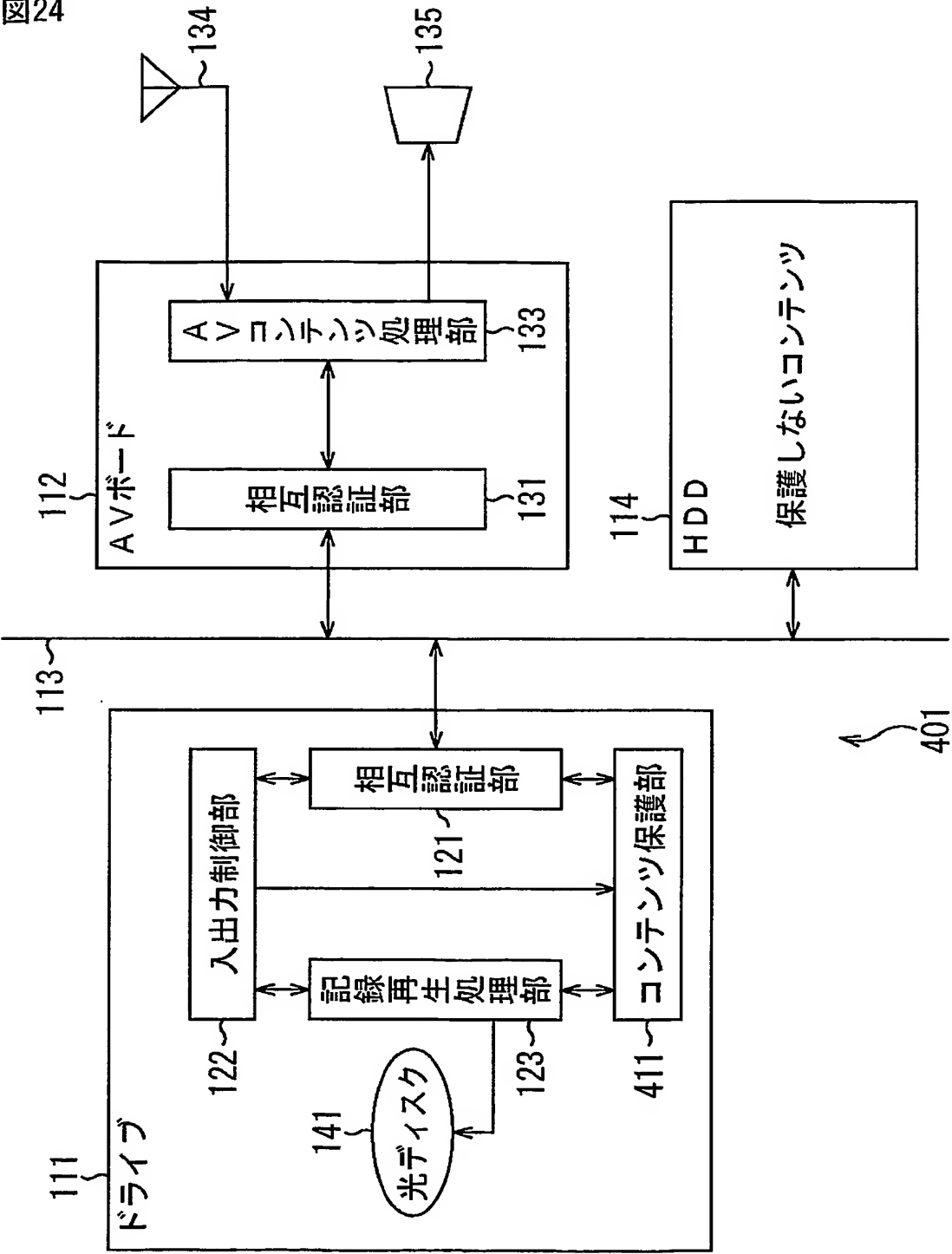
【図 23】

図23



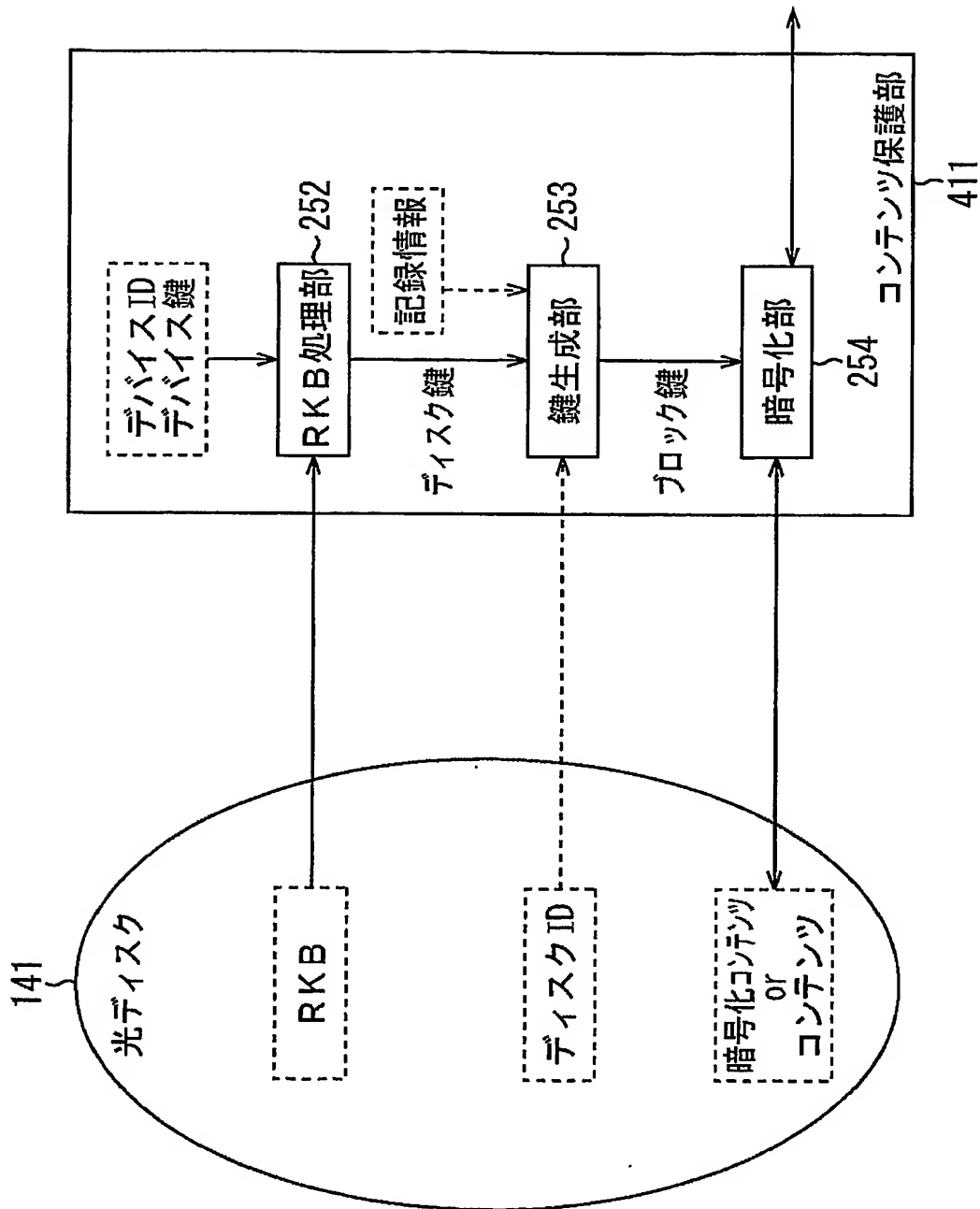
【図 24】

図24



【図 25】

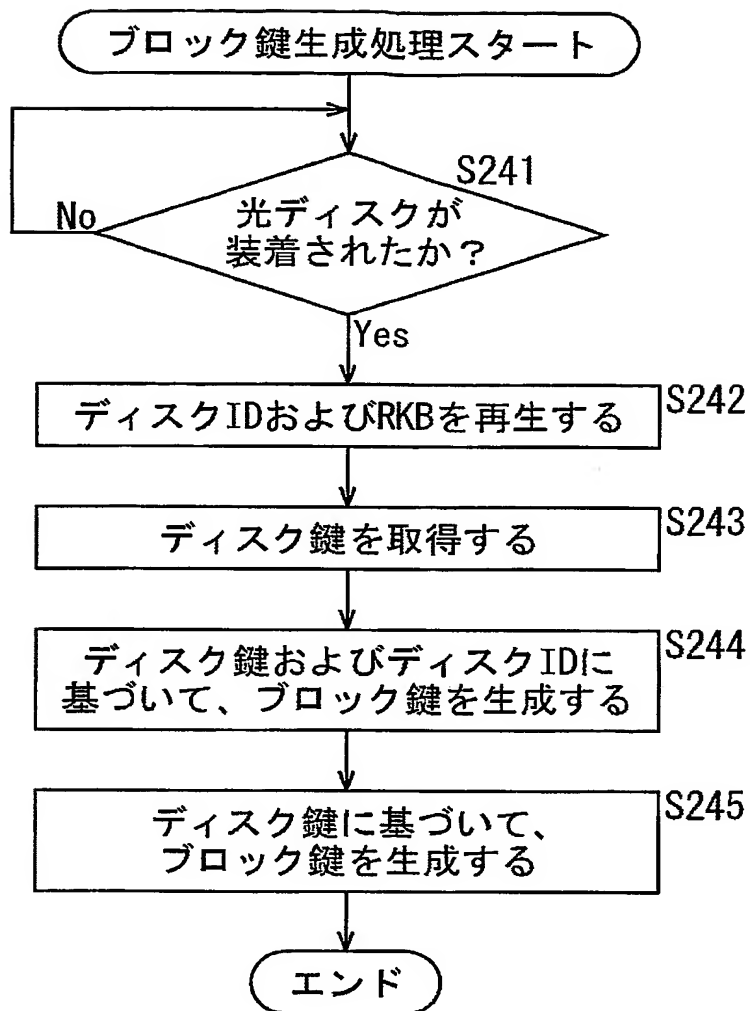
図 25





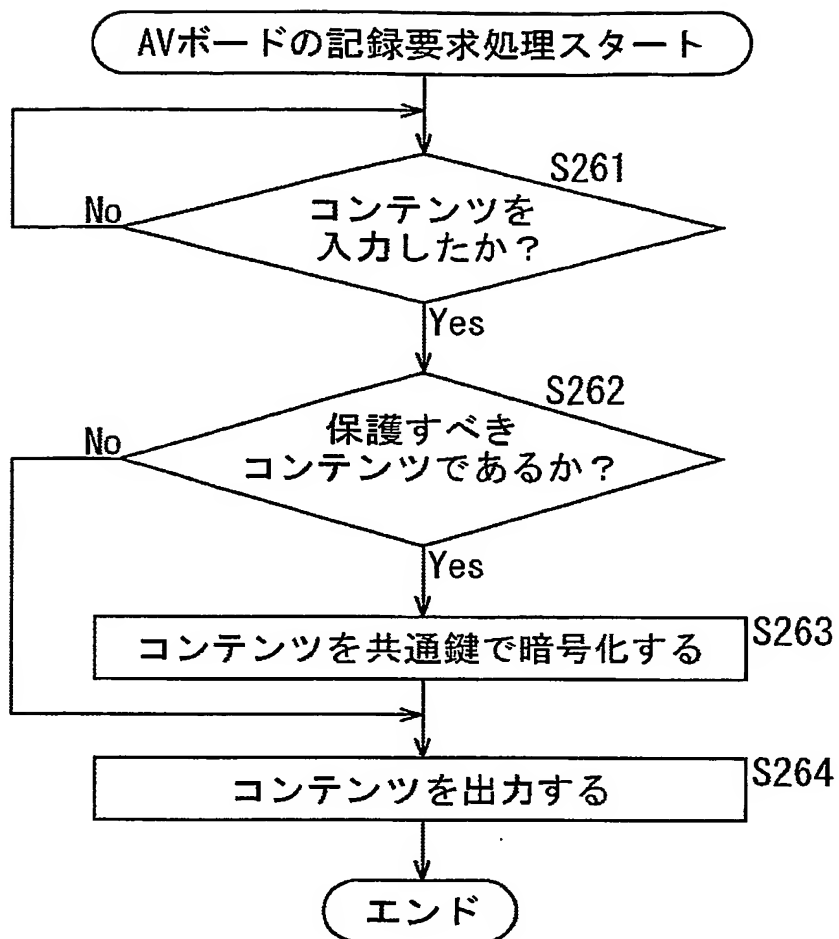
【図26】

図26



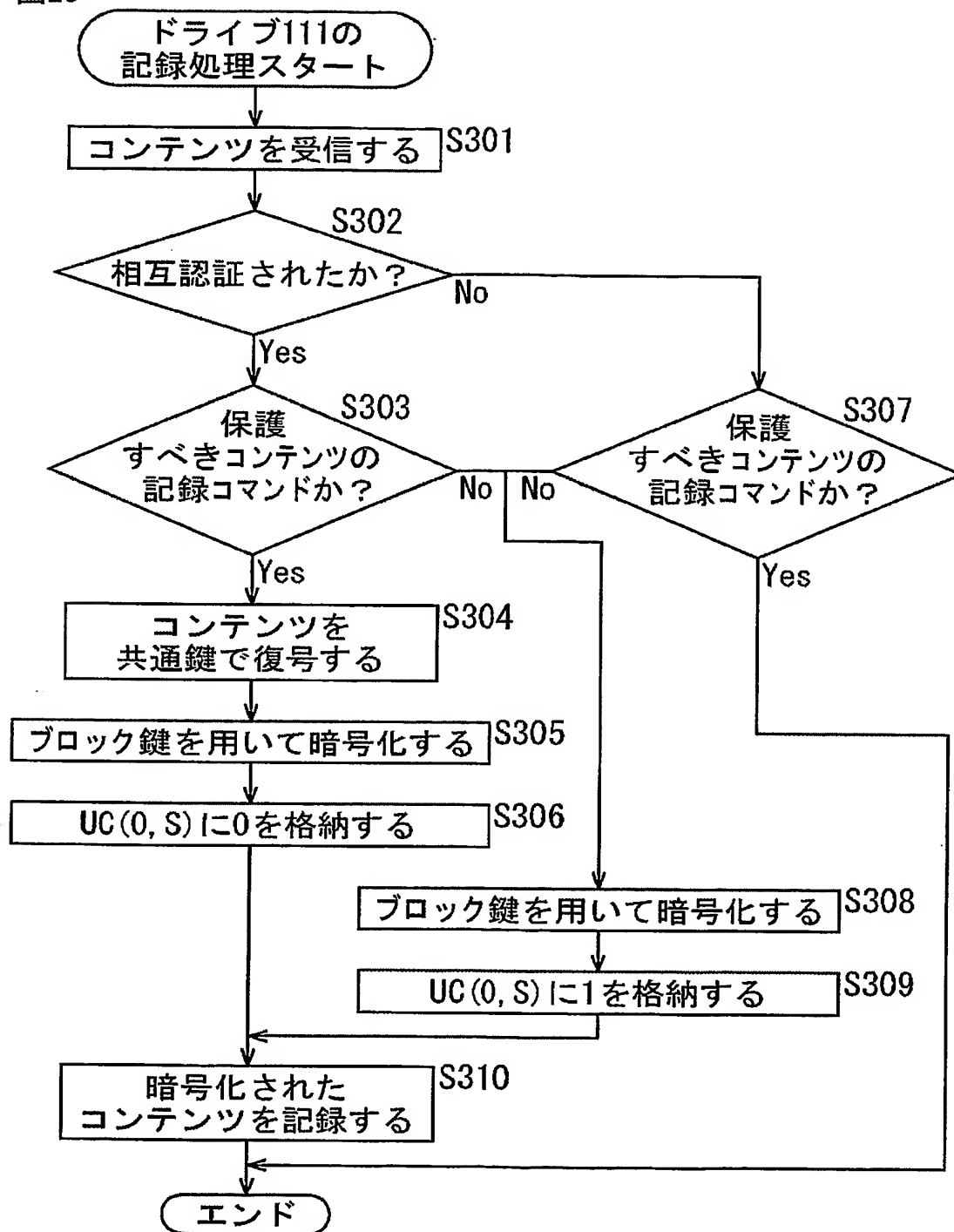
【図 27】

図27



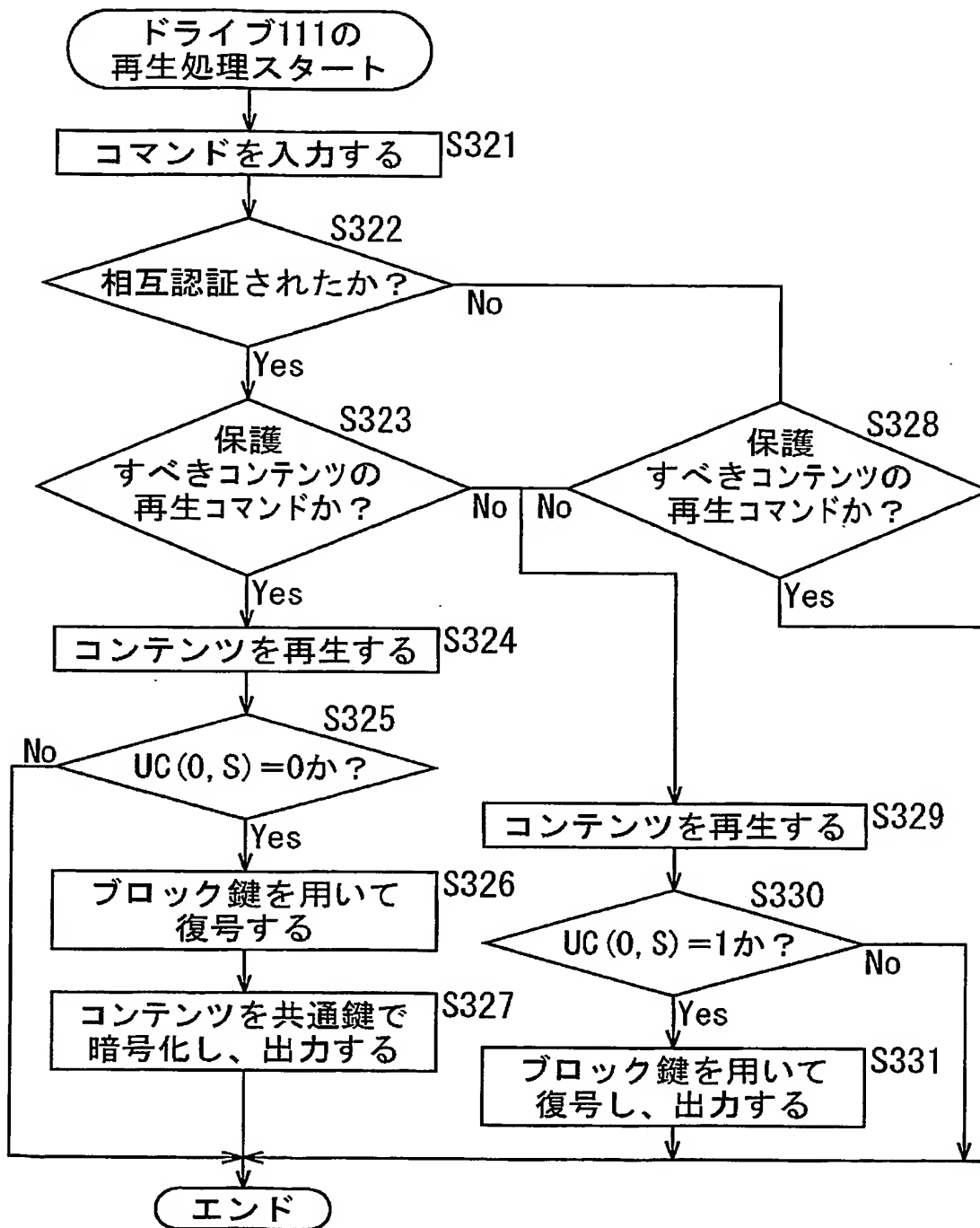
【図 28】

図28



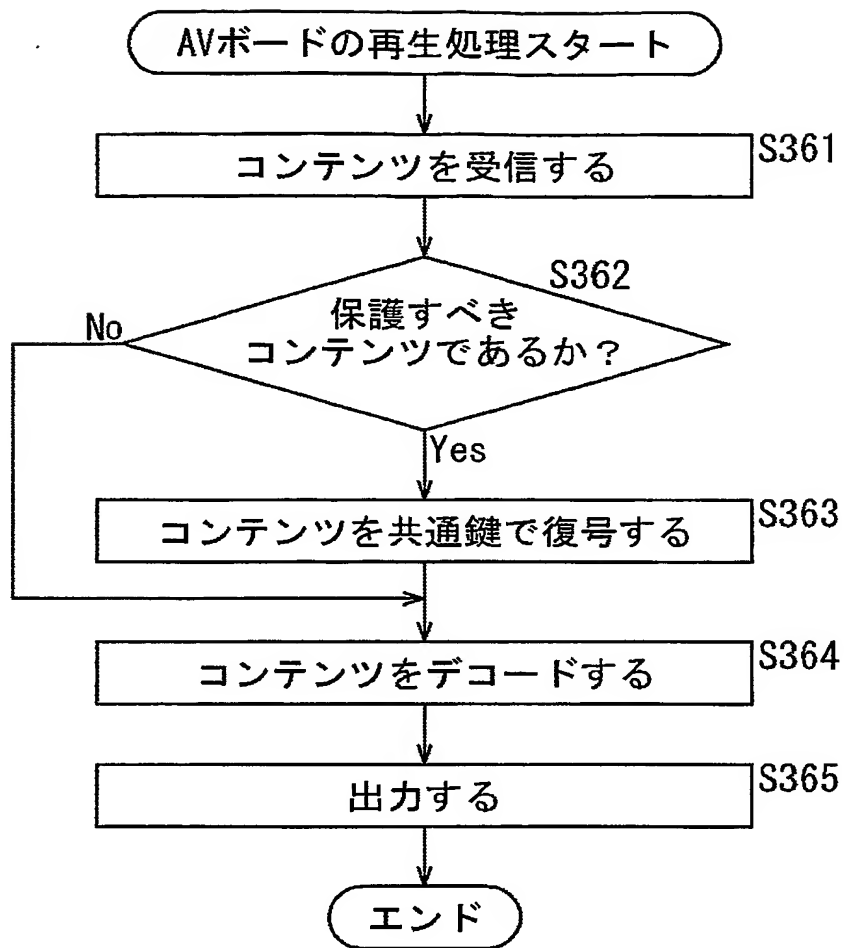
【図 29】

図29



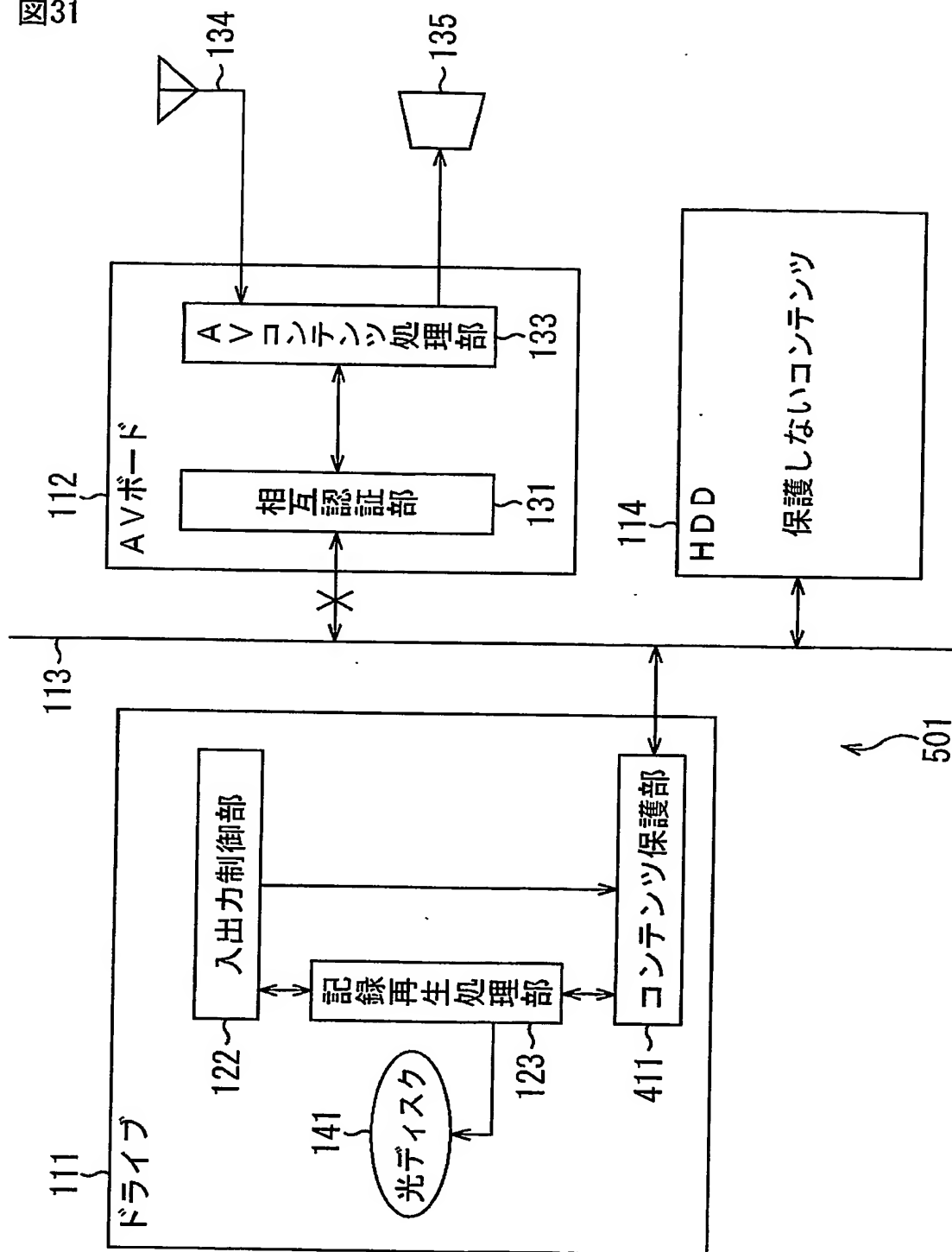
【図 30】

図30



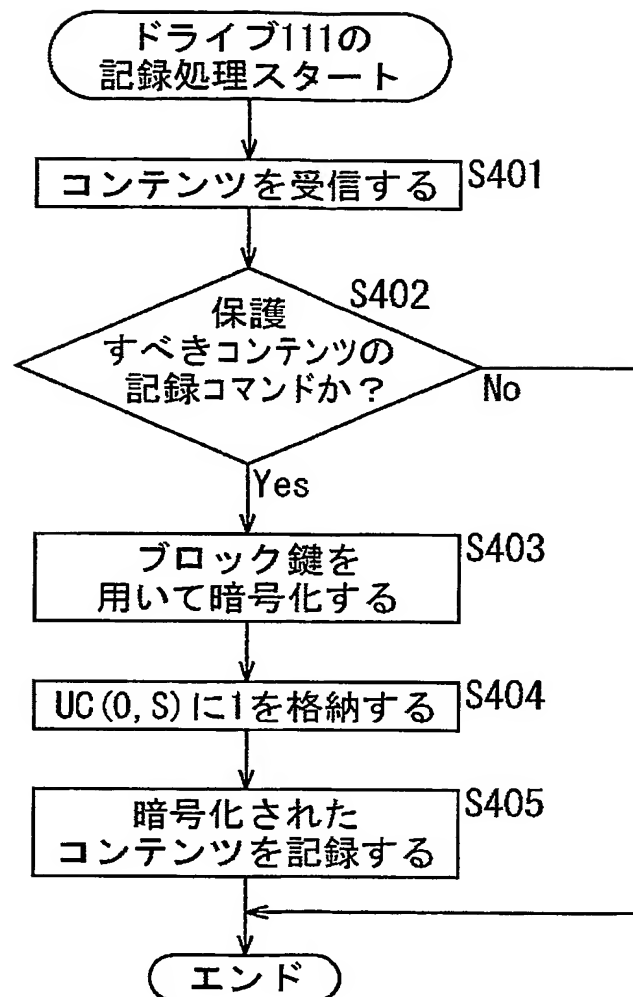
【図 31】

図31



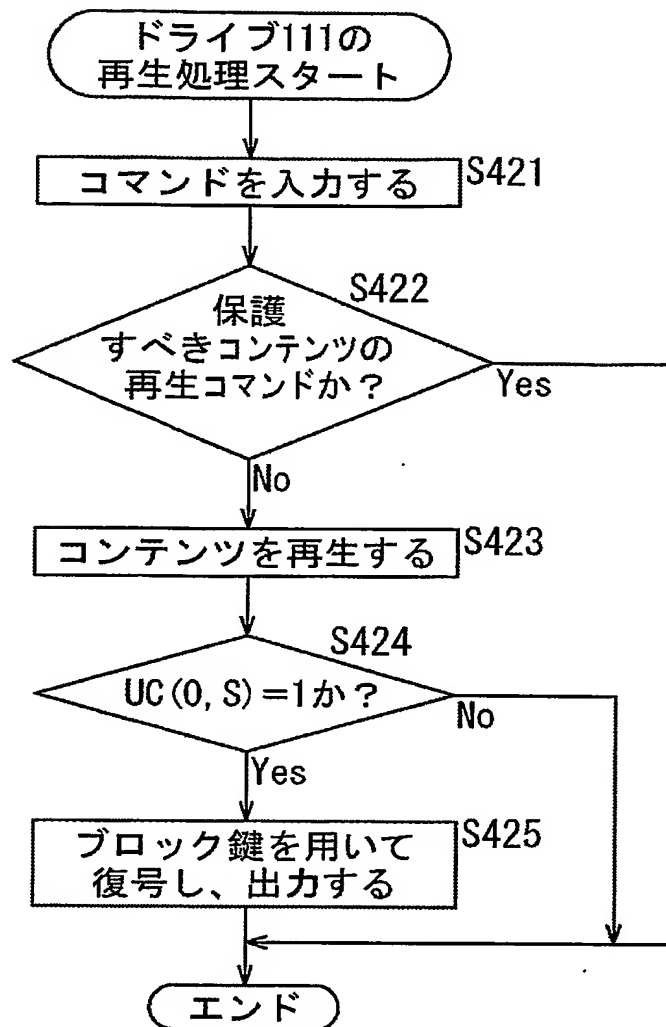
【図 32】

図32



【図 33】

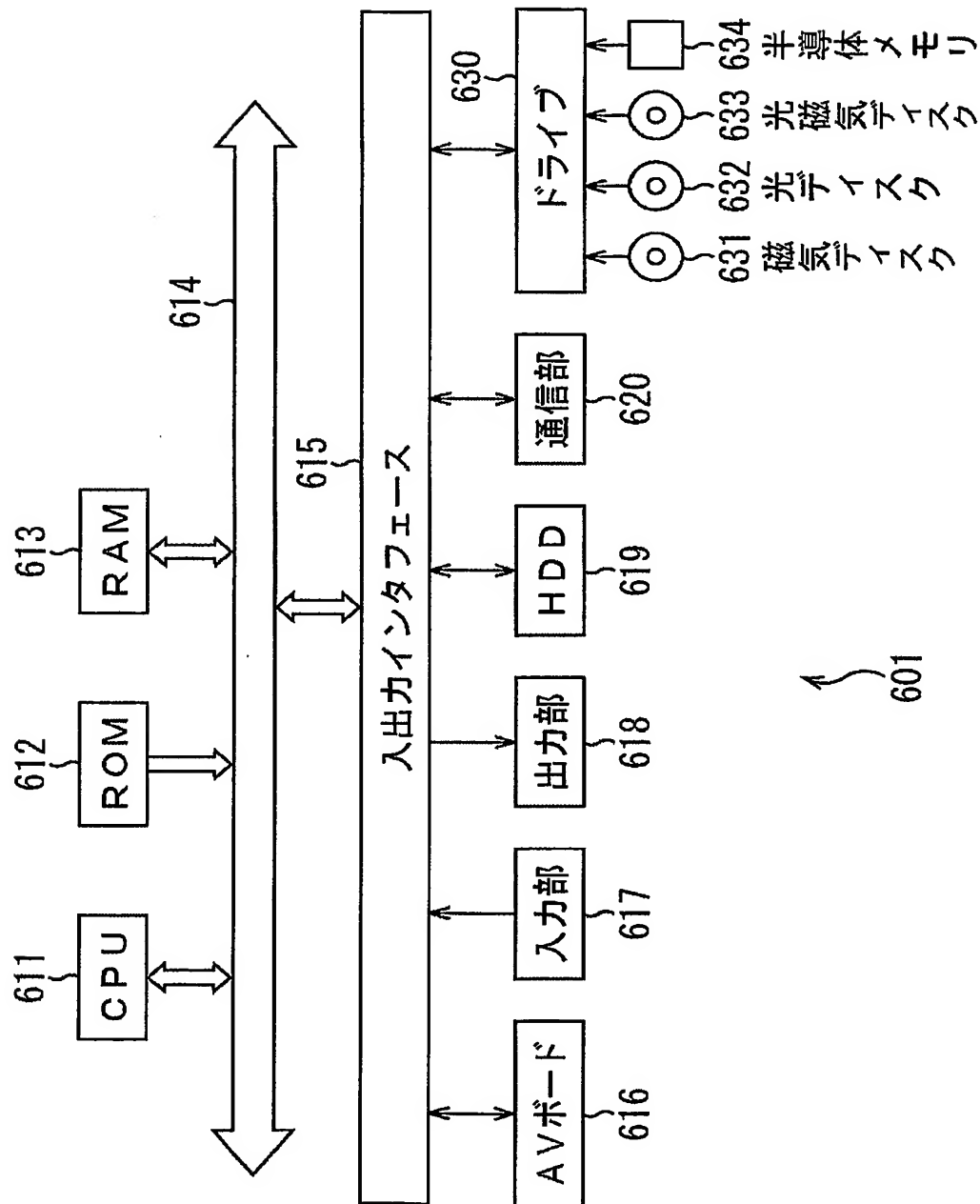
図33





【図 34】

図34



【書類名】 要約書

【要約】

【課題】 保護の要不要に基づいて、コンテンツを柔軟に保護することができるようにする。

【解決手段】 入出力制御部 1 2 2 は、相互認証部 1 2 1 により A V ボード 1 1 2 との間で相互認証がされ、かつ、相互認証部 1 2 1 に入力されたコンテンツが共通鍵で暗号化されている場合、バス 1 1 3 を介して入力されるコンテンツがバス 1 1 3 上で保護されるべきコンテンツであると判断し、記録再生処理部 1 2 3 を制御し、このコンテンツに対応するユーザコントロールデータの U C ( 0 , S ) に、バス 1 1 3 上で保護すべきコンテンツであるという保護情報「0」を生成させる。記録再生処理部 1 2 3 は、生成した保護情報を、コンテンツとともに、光ディスク 1 4 1 に記録する。本発明は、光ディスク記録再生装置に適用できる。

【選択図】 図 4

特願 2 0 0 2 - 3 3 6 7 5 4

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 2 1 8 5 ]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名

ソニー株式会社